U.S. Army War College
Dept. of Military Strategy,
Planning, and Operations
&
Center for Strategic
Leadership

November 2011
AY12 Edition

Information Operations Primer

Fundamentals of Information Operations

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
NOV 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Operations Primer	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College,Department of Military Strategy, Planning, and Operations ,122 Forbes Avenue,Carlisle,PA,17013**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**204**	

Middle States Accreditation

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

DEPARTMENT OF THE ARMY
UNITED STATES ARMY WAR COLLEGE AND CARLISLE BARRACKS
CARLISLE, PENNSYLVANIA 17013-5217

REPLY TO
ATTENTION OF

ATWC-A 19 October 2011

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: U.S. Army War College Information Operations Primer

This is a document prepared primarily for use by the staff, faculty, and students of the U.S. Army War College. However, U.S. Government (USG) agencies and organizations may reprint this document, or portions of it, without further permission from the U.S. Army War College. Further, USG agencies and organizations may post this document wholly, or in part, to their official approved websites. Non-Department of Defense or organization requests to reprint will be handled on a case-by-case basis.

William T. Johnsen
WILLIAM T. JOHNSEN, PH.D.
Dean of Academics

DISTRIBUTION:
DMSPO 500

This Page Intentionally Blank

Foreword

This latest revision of the Information Operations Primer provides an overview of Department of Defense (DoD) Information Operations (IO) doctrine and organizations at the joint and individual service levels. It is primarily intended to serve students and staff of the U.S. Army War College as a ready reference for IO information extracted and summarized from a variety of sources. Wherever possible, Internet websites have been given to provide access to additional and more up-to-date information. This booklet is intentionally UNCLASSIFIED so that the material can be easily referenced during course work, while engaged in exercises, and later in subsequent assignments.

This booklet begins with an overview of Information Operations, Strategic Communication and Cyberspace Operations. At each level it describes strategies or doctrine, agencies, organizations, and educational institutions dedicated to the information element of national power. Finally, the document concludes with an IO specific glossary and hyperlinks to information operations, cyberspace operations and strategic communication related websites.

Readers will note that many of the concepts, documents, and organizations are "works in progress" as DoD and the services strive to address the challenges of a rapidly changing IO environment. Thus, this summarization effort is on-going and continuous. Please address any suggested additions, revisions and/or corrections to the primary points of contact below for inclusion in subsequent editions.

The U.S. Army War College extends a special thanks and recognition to the individuals throughout the Department of Defense, uniformed military services, and Department of State whose help and assistance have made the revision of this Primer possible. We also thank Benjamin Leitzel for coordinating the inputs from over 30 organizations and Judy Sosa for proofreading and ensuring that this document is accurate and readable.

Department of Military Strategy, Planning, and Operations
U.S. Army War College
122 Forbes Avenue
Carlisle Barracks, PA 17013-5242
717-245-3491
carl_ATWC-ASP@conus.army.mil

Professor Dennis M. Murphy
Professor of Information Operations/
Information in Warfare
U.S. Army War College, Center for Strategic Leadership

This Page Intentionally Blank

Summary of Changes

The following changes have been made in this edition of the IO Primer:

Additions:

- U.S. International Strategy for Cyberspace
- DoD Strategy for Operating in Cyberspace
- The Center for Strategic Counterterrorism Communications
- Department of Defense Chief Information Officer
- Army Cyber Command

Deletions:

- The Assistant Secretary Of Defense – Networks and Information Integration (ASD(NII)). Replaced by Department of Defense Chief Information Officer.
- The Joint Military Information Support Command (JMISC) was deactivated and information on this organization was removed from the IO Primer.
- The Under Secretary of Defense for Intelligence (USD(I)) IO activities have been transferred to the Under Secretary of Defense for Policy (USD (P)).

Revisions:

- New Definition for Information Operations (IO) was added to the Glossary.
- The "Information Operations", "Strategic Communication" and "Cyberspace and Cyberspace Operations" sections have been updated.
- With a few exceptions, Department of Defense and Department of State agency sections have been updated where appropriate. Sections have been reviewed by the responsible office and most sections have some changes.

This Page Intentionally Blank

Table of Contents

I. CONCEPTS

This section includes an overview of the concepts and latest developments in:

- **Information Operations**
- **Strategic Communication**
- **Cyberspace and Cyberspace Operations**

Back to Table of Contents

This Page Intentionally Blank

Information Operations

Notes on Changes: This introduction examines Information Operations (IO) conceptually and doctrinally, but is intended only as a guide to facilitate academic discussion and is not authoritative. Both Army and Joint doctrine for Information Operations are being revised and will also be affected by the recent activation of U.S. Cyber Command. As of this writing, Joint IO and Cyberspace Operations doctrine are being developed in parallel with expected publication in summer 2012. While the information is current as of publication, readers should consult the following sites for updates and changes:

http://www.dtic.mil/whs/directives/corres/dir.html (DODD 3600.01, Information Operations)
http://www.dtic.mil/doctrine/new_pubs/jointpub_operations.htm (JP 3-13, Joint IO doctrine)
http://www.dtic.mil/doctrine/new_pubs/jointpub_reference.htm (Joint dictionary)
http://www.army.mil/usapa/doctrine/Active_FM.html (FM 3-0, Army Operations and FM 3-13, Army IO doctrine)

Background: Information Operations are an evolving construct with roots back to antiquity, thus it is both an old and a new concept. The late 1970's saw the emergence of Information Warfare (IW) and Command and Control Warfare (C2W) as war-fighting constructs integrating several diverse capabilities. These further evolved into Information Operations, recognizing the role of information as an element of power across the spectrum of peace, conflict, and war.

1. IO is an Integrating Function. Information Operations are the integration of capabilities involving information and information systems in order to gain a military advantage. This concept is similar to Joint Operations, which are the integration of service capabilities or Combined Operations, which are the integration of two or more forces or agencies of two or more allies. The integration envisioned is not mere deconfliction, but the synchronization of activities leading to action, and in turn, achieving desired effects that are significantly greater than the sum of the individual components.

2. Purpose of IO. Information Operations seek to influence the *behavior* of target audiences by changing their ability to make decisions, while simultaneously defending the friendly capability to make proper decisions. This is no different from the exercise of the other forms of national power. In this instance the means is information, but the resulting outcome is the same.

a. While frequently referred to as "soft-power" or "non-kinetic," IO includes the use of physical attack against adversary information systems or directly against decision makers. IO also employs technology-based activities to affect adversary information systems.

b. Affecting the target's decision cycle (sometimes referred to as his "OODA-loop" (observe, orient, decide, act - loop)) is a means of influencing target behavior. Obviously, reducing an adversary's ability to make timely and effective decisions will degrade his exercise of initiative or his response to friendly military action.

c. Action must also be taken to protect friendly information and information systems from compromise or disruption, since the U.S. military is particularly reliant on these systems to maintain situational awareness, support decision making and to command and control forces. These protective actions are not intended to prevent the unrestricted flow of information vital to a free society, but rather to prevent a target's manipulation or distortion of information or attacks on information systems from being effective.

3. The Information Environment and Communication. At this point, it would be helpful to conceptualize the kind of activities, which would be effective in achieving the desired results of influencing target behavior while protecting friendly capabilities.

a. All Information Operations activities occur within the broader context of the information environment. This environment recognizes the critical role that information and information systems play in today's advanced societies as they progressed along a continuum from agrarian, to industrial, to the information age. This environment pervades and transcends the boundaries of land, sea, air, space, and cyberspace. It is accessible and leveraged by both state and non-state actors.

b. Within this environment there are three conceptual dimensions of connectivity, content and cognitive.

(1) "Connectivity" refers to the physical or electronic links, which enable information to flow and includes those non-technical relationships between people.

(2) The "content" is comprised of the words, images, databases, etc. that contain the information itself, as well as actions and inactions to which meaning is ascribed. This dimension links the physical real world with the human consciousness of the cognitive dimension both as a source of input (stimulus, senses, etc.) and to convey output (intent, direction, decisions, etc.).

(3) The "cognitive" dimension exists in the mind. This is where the individual processes the received information according to a unique set of perceptions (interprets the information), opinions (within a greater context of how he sees the world organized), and beliefs (on a foundation of core central values). These attributes act as a "window" to filter the information and provide a sense of meaning and context. The information is evaluated and processed to form decisions, which are communicated back through the information dimension to the physical world. It should be noted that the cognitive dimension cannot be directly attacked (short of mind-altering drugs) but must be influenced indirectly through the physical and information dimensions.

c. Information Operations impact the three dimensions of the information environment through a variety of capabilities. Electronic warfare and computer network attack both disrupt connectivity, while Soldier and leader engagement enhances connectivity. Military Information Support Operations, public affairs, and Soldier and leader engagement all provide content, while computer network operations can modify content, and units and individual Soldiers provide the most credible content through their actions. While Information Operations cannot modify human mental processing that occurs in the cognitive dimensions, it can apply computer network operations to alter the automated information processing systems.

d. While the information environment describes the context in which we work, it does not fully explain the process that occurs as messages move across that environment and factors that can influence the outcome. Some of the factors that influence can be explained by theoretical models of communication, such as Berlo's model,[1] represented in Figure 1.

(1) Berlo's model illustrates how various factors can modify information in a message at both the source and receiver's end of the communication process. This is particularly significant for the military, since there may be significant differences in the culture and social systems of the individuals or organizations involved. In his pragmatic communication model, Dr. Rich Rowley points out that the history of interactions and expectations for the future also influence the communication process.[2] "The little boy who cried wolf" is an obvious, if quaint, example of how a history of interactions can influence a receiver to ignore an otherwise timely and accurate message.

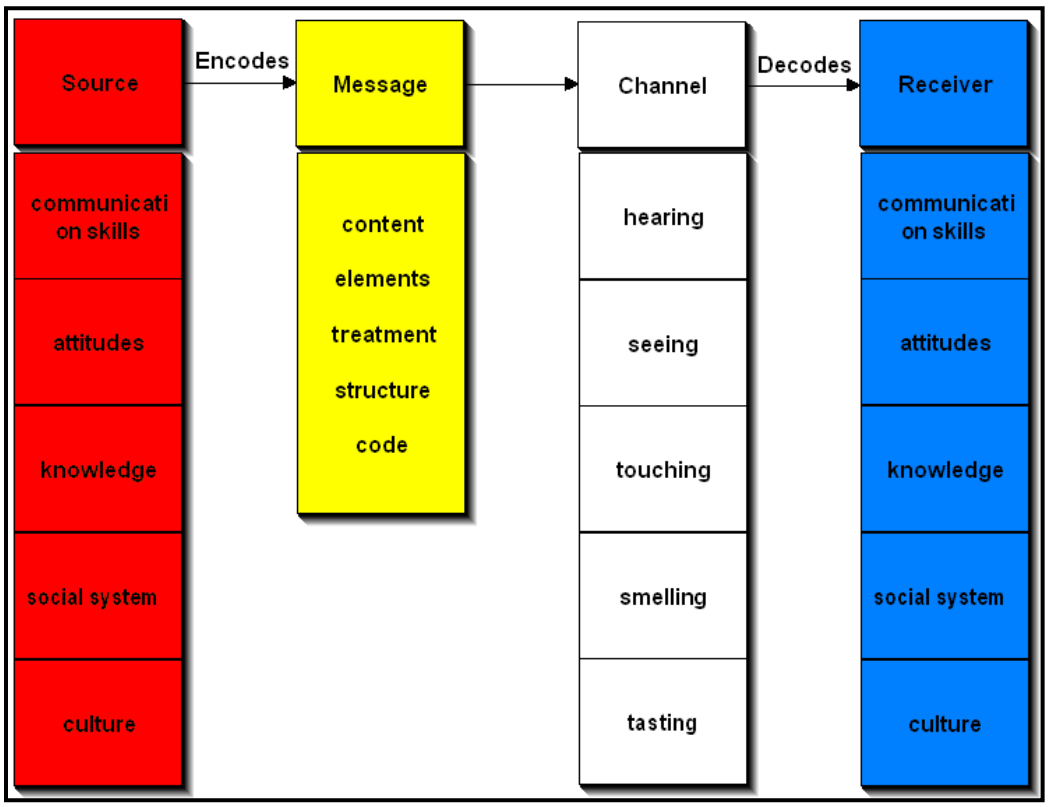


Figure 1. Berlo's Model of Communication

(2) Just as information operations can apply various capabilities to influence the information environment, these capabilities account for subtleties in the communication process when developing messages and when executing operations to convey these messages. These influences can be as elementary as using audio communications means with illiterate receivers, or as complex as accounting for the political influence of sub-tribal cultures when communicating in rural Afghanistan.

4. <u>IO Definition.</u> The Secretary of Defense directed a significant change to the joint definition of IO in a January 2011 memorandum: IO is "The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own." The memo further describes the reason for this change. The previous definition listed five core capabilities within it. Often this resulted in an emphasis on the capability at the expense of recognizing IO as an integrating function. It further led to the perception of IO ownership of the capabilities. Removing the capabilities makes it clear that, as an integrating function, IO owns nothing. Furthermore, by explicitly excluding a laundry list of

capabilities, the definition is no longer self-limiting since the tools available are now constrained only by the imagination of the commander and his staff. While it may not be about everything you do, it certainly can be about anything you can do to achieve the desired information effects in support of military operations, to include physical attack, i.e. actions.

5. Traditional Capabilities. This section will define and explain what were previously referred to as core capabilities of IO. While removed from the new definition of IO, current plans are to address them in the body of the doctrine currently under revision. Consequently, they are covered here as well. Remember that these are not a limiting list, since the new definition leaves "information-related capabilities" intentionally open-ended.

a. **Military Information Support Operations (MISO)** are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of MISO is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.

b. **Military Deception (MILDEC)** consists of actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or fail to take actions) that will contribute to the accomplishment of the friendly mission.

c. **Operations Security (OPSEC)** is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

(1) Identify critical information that would harm the organization's ability to effectively carry out normal operation if obtained by an adversary.

(2) Analyze the threat to determine the adversary's capabilities, use for the information, determination, and resources.

(3) Analyze the vulnerabilities by viewing the organization from the adversary's perspective, especially in terms of physical safeguards, network/electronic safeguards and personnel training, which are in place to protect the critical information.

(4) Identify vulnerabilities, which the adversary can exploit by matching the adversary's capabilities to the vulnerabilities, which have been identified.

(5) Identify and enact countermeasures to lower or eliminate the risk.

d. **Electronic Warfare (EW)** is any military action involving the use of electromagnetic and directed energy to dominate the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are as follows:

(1) Electronic Attack (EA)**.** That division of electronic warfare involving the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams).

(2) Electronic Protection (EP)**.** That division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of

friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability.

(3) Electronic Warfare Support (ES). That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Thus, electronic warfare support provides information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Electronic warfare support data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence.

e. **Computer Network Operations (CNO).** Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. Upcoming revisions to Joint doctrine will likely move these capabilities under cyberspace operations, which are discussed in a later chapter of the primer, but since the IO section will continue to coordinate with these efforts, they are defined here as well.

(1) Computer Network Attack (CNA). Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

(2) Computer Network Defense (CND). Actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks.

(3) Computer Network Exploitation (CNE). Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.

f. Current doctrine also addresses "supporting" capabilities and "related capabilities." ***Supporting Capabilities*** provide additional operational effects: Information Assurance (IA), Physical Security, Physical Attack, Counterintelligence (CI), and Combat Camera (COMCAM). ***Related Capabilities*** of Public Affairs (PA), Civil-Military Operations (CMO), and Defense Support to Public Diplomacy (DSPD) contribute to the accomplishment of the IO mission. These activities often have regulatory, statutory, or policy restrictions and limitations regarding their employment, which must be observed.

6. IO Planning and Execution. Having identified the purpose of IO, its definition, and some of the associated traditional activities, this section will address how IO capabilities are integrated.

a. Information Operations are planned by the IO section of a joint or service staff under the direction and supervision of a designated IO officer. Within a joint command, such as a Combatant Command, this section normally resides within the operations directorate (J-3) of the staff, often designated the J-39. Appropriate representatives from information-related capabilities as well as the special staff, service/functional components, and appropriate national agencies serve as members of the J-39.

b. IO planning must be fully integrated into the overall joint planning process, be it deliberate or crisis action. There should not be a separate "IO campaign plan" just as there is no separate "maneuver campaign plan." Additionally, visualizing "information" as a separate Line of Operation (LOO) does improve visibility of IO, but it is at the cost of obscuring how (or whether) IO has properly coordinated support to the other LOOs. Commanders who describe and visualize IO as something separate will likely find that it becomes something separate.

c. Products from the IO planning process are incorporated into the Commander's Estimate, Commander's Concept, and the OPLAN/OPORD as documented in the Joint Operation Planning and Execution System (JOPES).

d. Evaluation of the success of the execution of the plan is done through identified measures of effectiveness (MOE), which is how well the plan achieved the desired result, and measures of performance (MOP), which is how well the plan was executed. MOE and MOP must be identified as a component of the IO planning process based upon realistic expectations for timeliness and accuracy of data received.

7. Current Issues.

a. The current policy discussion of whether information operations constitute traditional military activities will affect the future of IO. (Note the inclusion of "during military operations" in the new definition, which was not part of the previous definition.) Part of this discussion centers around attribution of MISO products, and part around computer network attack and the authorities that cover these activities. Additionally, the military's activities to influence target audiences outside combat zones has sparked debate over whether these activities should properly fall under the Department of State. These questions have caused additional media interest and Congressional scrutiny, and in cases have resulted in reduced funding for military IO efforts. As of this writing DoD continues to focus on codification and understanding of IO as a traditional military activity within the greater national security community.

b. U.S. Army doctrine regarding IO has recently changed. Field Manual 6-0, *Mission Command*, (June 2011) established the new Mission Command warfighting function and launched the Army's evolution of information operations to Inform and Influence Activities (IIA). These activities support and enhance current joint information operations doctrine that, by definition, remains focused on adversaries and potential adversaries only. Inform and Influence Activities focus on all audiences within the information environment, which include domestic, foreign friendly and neutral, adversary and enemy. It is also in line with the new definition for IO and emerging joint doctrine as it also enables commanders with multiple information-related capabilities and allows them to evaluate and use available internal and request external resources to inform or influence selected populaces, actors or audiences as desired to support his or her mission objectives. Inform and Influence Activities are integrated by the G-7.

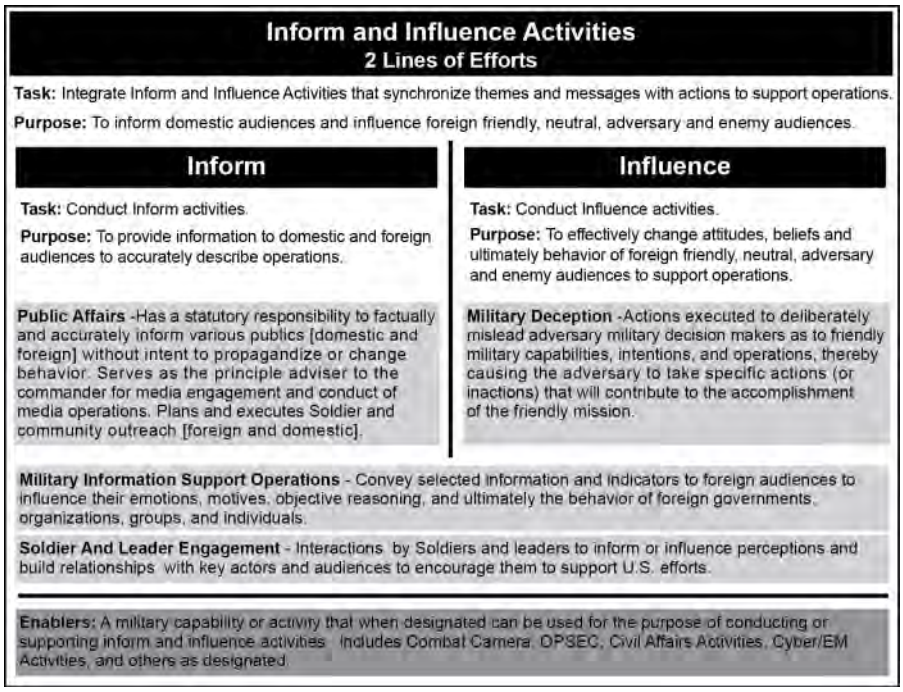


Figure 2. Army Inform and Influence Activities.

c. Recognizing the importance of operations in cyberspace, draft Army doctrine labels the CNO and EW capabilities presented in the joint discussion above as falling within the newly-defined area of "Cyber/Electromagnetic Activities." This construct is presented in Figure 3. In Army organizations, the G-7 will not have the responsibility for synchronizing all Cyber/EW Activities but will conduct coordination to ensure these activities support IIA activities.

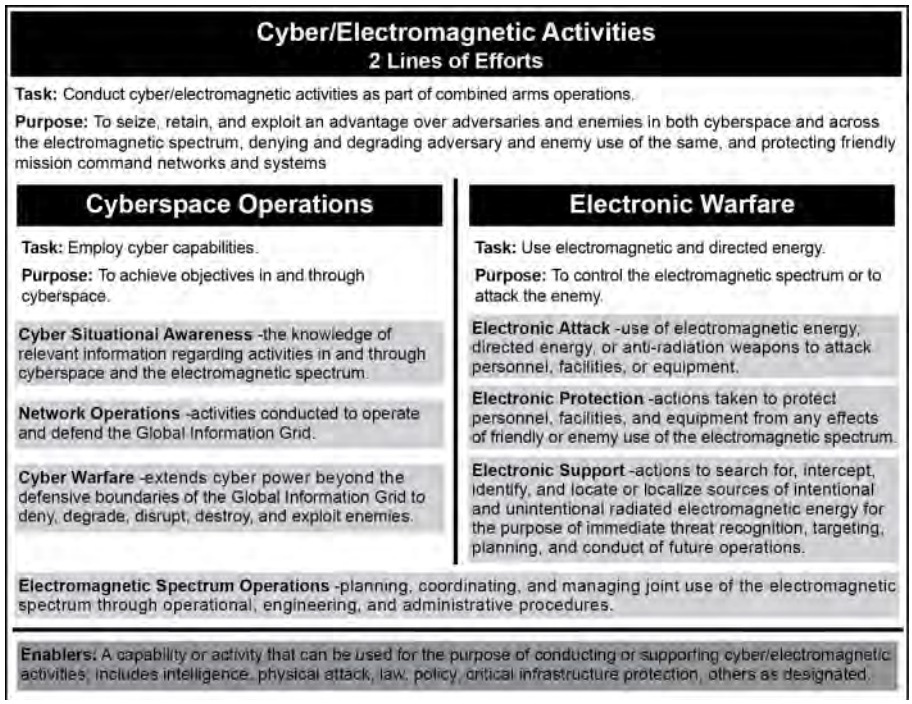


Figure 3. Army Cyber/Electromagnetic Activities

8. Additional Considerations.

a. Personal interactions are perhaps the most important means to influence a target audience. In the context of persuasive influence, these interactions can range from compulsion and coercion on one end of the spectrum to cooperation and collaboration on the other. Viewed in the terms of the amount of planning involved, they can vary from deliberate meetings between a carefully chosen messenger and an influential target covering specific issues, or chance meetings between military service members and random members of the populace.

b. Regardless of how the message is transmitted, the credibility of our messages and messengers is key to the effectiveness of our influence efforts. We must recognize that we lose credibility when the implied messages of our actions do not match the messages of our overt communications. If these messages are not coordinated during the IO planning process, our credibility and effectiveness suffer. This shortfall is often referred to as the "say-do" gap.

c. An appropriate understanding of the target's culture and norms is essential to effective information operations. Our communications efforts must avoid the tendency to "mirror" friendly cultural values and perspectives, but rather must be prepared, executed and evaluated from the perspective of the target audience, through their cultural lens (it's how the message is received that matters). This often means that the U.S. is not the appropriate messenger. Rather, encouraging a credible indigenous key influencer to send the message might be a better option.

d. Even when done effectively, IO effects typically take longer to achieve and are more difficult to measure than conventional operations. Therefore, a long term commitment to building relationships and maintaining communication through a two-way dialog is critical. Theater Security Cooperation Plans are a vital part of this effort. Waiting until a crisis occurs and then "throwing info ops at it" is an exercise in futility.

Effective IO leverages the power of information to complement the other instruments of national power resulting in the achievement of national objectives with less expenditure of blood and treasure.

Dennis M. Murphy
Professor of Information Operations and Information in Warfare
U.S. Army War College

Endnotes

[1] David K. Berlo, *The Process of Communication: An Introduction to Theory and Practice* (New York: Holt, Rinehart and Winston, 1960), 72.
[2] Richard D. Rowley, "Pragmatic Communication Model," 1999, http://www.aligningaction.com/prgmodel.htm (accessed 14 October 2010).

Strategic Communication

Strategic Communication. This section addresses some considerations of the information element of power at the national and theater strategic level.

1. Information and National Power. Interestingly, one needs to go back to the Reagan administration to find the most succinct and pointed mention of information as an element of power in formal government documents.[1] Subsequent national security documents allude to different aspects of information but without a specific strategy or definition. Still, it is generally accepted in the United States government today that information is an element of national power along with diplomatic, military and economic power … and that information is woven through the other elements since their activities will have an informational impact.[2] Given this dearth of official documentation, Drs. Dan Kuehl and Bob Nielson proffered the following definition of the information element: "use of information content and technology as strategic instruments to shape fundamental political, economic, military and cultural forces on a long-term basis to affect the global behavior of governments, supra-governmental organizations, and societies to support national security."[3] Information as power is wielded in an increasingly complex environment consisting of physical, information, and cognitive dimensions.

2. Strategic Communication Overview. The executive branch of the U.S. government has the responsibility to develop and sustain an information strategy that ensures strategic communication occurs consistent with and in support of policy development and implementation. This strategy should guide and direct information activities across the geo-strategic environment. Effective strategic communication is the desired "way" (given the "ends, ways, means" model) that information is wielded in accordance with that strategy. The U.S. government provided the first national level definition of strategic communication in a report to Congress in March 2010: "[Strategic communication] is the synchronization of our words and deeds as well as deliberate efforts to communicate and engage with intended audiences."[4] The Department of Defense maintains a separate but related definition: "focused United States Government efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of United States Government interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power." Parsing these to their essentials, strategic communication is the orchestration of actions, images and words to achieve cognitive effects in support of policy and military objectives. While the capabilities used to achieve those effects should be unconstrained, primary supporting capabilities of strategic communication at the national strategic level are generally considered as Public Affairs (PA), military Information Operations (IO), and Public Diplomacy (PD).

a. Public affairs and military IO have been defined in the context of their use within the Department of Defense (DOD) in the previous section.

b. Public diplomacy is primarily practiced by the Department of State (DOS). It is defined as "those overt international public information activities of the United States Government

designed to promote United States foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers, and by broadening the dialogue between American citizens and institutions and their counterparts abroad."[5]

c. International broadcasting services are cited as a strategic communication means in some definitions. The Broadcasting Board of Governors (BBG) includes all U.S. civilian international broadcasting. This includes Voice of America (VOA), Radio Free Europe/Radio Liberty, Radio Free Asia, Radio and TV Marti, and the Middle East Broadcasting Networks (Radio Sawa and Alhurra Television). VOA increasingly uses the Internet, mobile devices, social media and other digital platforms.[6]

Strategic communication is considered by some to be solely a national strategic concept; however, it is increasingly recognized as occurring at all levels from tactical to strategic, despite the lexicon of the term itself.

3. History of Strategic Communication. While "strategic communication" is a fairly new term in U.S. government parlance, the concept, theory, and practice behind it is not. Winfield Scott recognized the importance of strategic communication at the theater level in Veracruz in 1847. Realizing the influence of the Catholic Church on Mexican society, Scott attended Mass with his staff at the Veracruz Cathedral to display the respect of U.S. forces. He further ordered U.S. soldiers to salute Mexican priests in the streets. Each of these measures was "part of a calculated campaign to win the friendship of the Mexicans."[7]

The recent history of national strategic communication shows concerted efforts to positively portray the U.S. story in order to persuade and influence.

a. The Committee on Public Information (1917), also known as the Creel Committee after its chief, newspaperman George Creel, sought to rally U.S. public opinion behind World War I on behalf of the Wilson administration. Its focus was the domestic audience and it used public speakers, advertising, pamphlets, periodicals, and the burgeoning American motion picture industry.

b. The Office of War Information (1942) focused both domestically and overseas, with broadcasts sent in German to Nazi Germany. The Voice of America (VOA) began its first broadcast with the statement, "Here speaks a voice from America. Every day at this time we will bring you the news of the war. The news may be good. The news may be bad. We shall tell you the truth."

c. The Smith-Mundt Act (1948) (actually, "The U.S. Information and Educational Exchange Act (Public Law 402; 80th Congress)"), established a statutory information agency for the first time in a period of peace with a mission to "promote a better understanding of the United States in other countries, and to increase mutual understanding" between Americans and foreigners. The act also forbade the Voice of America to transmit to an American audience. It is worth noting that Smith-Mundt is often cited today as the basis to limit the use of government information activities to influence since it may result in "propagandizing" the American public. This, of course, is complicated by the inevitable "blowback" or "bleedover" of foreign influence activities based on the global information environment.[8]

d. The United States Information Agency (USIA) (1953) was established by President Eisenhower as authorized by the Smith-Mundt Act. It encompassed all the information programs, including VOA (its largest element), that were previously in the Department of State, except for the educational exchange programs, which remained at State. The USIA Director reported to the President through the National Security Council and received complete, day-to-day guidance on U.S. foreign policy from the Secretary of State.

e. A 1998 State Department reorganization occurred in response to calls by some to reduce the size of the U.S. foreign affairs establishment. (This is considered the State Department's "peace dividend" following the Cold War.) The act folded the USIA into the Department of State. It pulled the Broadcasting Board of Governors out of USIA and made it a separate organization. The USIA slots were distributed throughout the State Department and its mission was given to the Bureau of International Information Programs.

4. National Strategic Communication - Current Models and Processes. The demise of USIA is generally regarded (in retrospect) as diluting the ability of the United States to effectively promulgate a national communication strategy, coordinate and integrate strategic themes and messages, and support public diplomacy efforts worldwide.[9] Additionally, organizations and processes have experienced great flux in recent years. Strategic communication efforts under the George W. Bush administration provided mixed results. While some interagency committees and offices were ineffective or became dormant, there was progress under Ambassador Karen Hughes (who assumed duties as the Under Secretary of State for Public Diplomacy and Public Affairs in the early fall of 2005 and departed in late 2007). The Under Secretary helps ensure that public diplomacy (described as engaging, informing, and influencing key international audiences) is practiced in harmony with public affairs (outreach to Americans) and traditional diplomacy to advance U.S. interests and security and to provide the moral basis for U.S. leadership in the world.[10] Ambassador Hughes provided specific guidance to public affairs officers at embassies throughout the world that either shortcut or eliminated bureaucratic clearances to speak to the international press. She established a rapid response unit within the State Department to monitor and respond to world and domestic events. She reinvigorated the Strategic Communication Policy Coordinating Committee and established communication plans for key pilot countries. And she established processes to disseminate coordinated U.S. themes and messages laterally and horizontally within the government. Finally, and perhaps most importantly, a long awaited National Strategy for Public Diplomacy and Strategic Communication was published under her leadership in May 2007.

The Obama administration's efforts to advance strategic communication efforts appear to be reaching steady state as of this writing. While the national strategy developed under the previous administration is no longer an active document, President Obama has issued a "National Framework for Strategic Communication" in response to a Congressional requirement. While not a strategy, per se, this document provides the first US government definition of strategic communication and outlines the organizations and processes to implement it at the national level. A Global Engagement and Strategic Communication Interagency Policy Committee was initially active but has recently become dormant with a shift of focus on very specific and localized grass roots efforts to combat violent extremism overseas. In light of this shift, a Center for Strategic Counterterrorism Communication (CSCC) was formally codified by Presidential Executive Order to "coordinate, orient, and inform Government-wide public communications activities directed at audiences abroad and targeted against violent extremists and terrorist organizations, especially al-Qa'ida and its affiliates and adherents, with the goal of using communication tools to reduce radicalization by terrorists and extremist violence and terrorism that threaten the interests and national security of the United States."[11] The CSCC replaces the operational level Global Strategic Engagement Center at State.

Judith McHale was sworn in as Under Secretary of State for Public Diplomacy and Public Affairs on 26 May 2009. Ms. McHale published her own strategic framework for public diplomacy entitled "Strengthening U.S. Engagement with the World." That document calls for the linkage of public diplomacy efforts to foreign policy objectives. It directs the redistribution of funding based on national priorities and the assignment of Deputy Assistant Secretaries of State for Public Diplomacy in each of the regional bureaus, among other initiatives. Under Secretary McHale

resigned her position to return to the private sector in July 2011. Assistant Secretary Ann Stock assumed the authorities of the Under Secretary for Public Diplomacy and Public Affairs on July 8, 2011. She previously led the Bureau of Educational and Cultural Affairs under McHale's office.

The Defense Department (DoD) has responded to the challenges posed by the current information environment but also with mixed results. The 2006 Quadrennial Defense Review (QDR) conducted a spin-off study on strategic communication that resulted in a roadmap addressing planning, resources and coordination.[12] Actions to achieve roadmap milestones are no longer formally monitored. However, in response to the same Congressional directive that produced the "National Framework for Strategic Communication," DoD produced a "Report on Strategic Communication" in December 2009. There they significantly noted that "Emergent thinking is coalescing around the notion that strategic communication should be viewed as a process, rather than as a set of capabilities, organizations, or discrete activities."[13] Still enduring are "Principles of Strategic Communication" published by the office of the Assistant Secretary of Defense (Public Affairs) in 2008.[14]

The Joint Staff has moved forward with a first draft of strategic communication doctrine. As of this writing, however, it appears that the progress of that document will be delayed until a Department of Defense Instruction (DoDI) is completed, thus providing a policy basis for the subordinate doctrinal manual. This DoD Instruction is still in an embryonic stage.

5. Theater Strategic Communication. Theater strategic communication receives only brief discussion in current doctrine. However, because of the importance of the information element of power in the current military campaigns in Iraq and Afghanistan, combatant commanders have established processes and organizations to address the need. Various organizational models exist among the combatant commands from separate strategic communication directorates to incorporation of strategic communication processes into effects cells. As of June 2010, it appeared that an organization consisting of a strategic communication director with small coordination staff and supporting strategic communication working group was becoming the norm.[15] As indicated above, the emergence of a DoD Instruction on strategic communication is a hopeful sign that specific doctrine for the concept will soon emerge.

While national strategic communication lists principal capabilities of PA, PD and IO, DoD strategic communication (and thus combatant command strategic communication) includes military PA, defense support to public diplomacy (alternately referred to as military support to public diplomacy), aspects of IO, principally PSYOP (recently changed to "MISO" or Military Information Support Operations), Military Diplomacy (MD) and Visual Information (VI).[16] The concept of defense support to public diplomacy is still vaguely defined with examples ranging from theater web initiatives aimed at certain regions and demographics within those regions to theater logistical support to embassies and diplomatic staffs. Military Diplomacy includes traditional interactions between U.S. senior military leaders and foreign military leaders. Beyond the importance of theater strategic communication in ongoing military operations, doctrine is correct to point out the importance of strategic communication activities in implementing theater security cooperation plans (TSCPs) based on its inherent shaping and deterrence capability.[17]

6. Ends, Ways, Means: Where Does Strategic Communication Fit? Strategists use a model of "ends, ways and means" to describe all aspects of a national or military strategy. Strategy is about how (the way) leaders will use the capabilities (means) available to achieve objectives (ends).[18] Understanding and engaging key audiences is meant to change perceptions, attitudes and ultimately behaviors to help achieve military (and in turn national) objectives. Thus, parsing the DoD definition it is apparent that strategic communication is a "way" to achieve an information effect on the cognitive dimension of the information environment (the required

"end"). The recent emphasis on strategic communication as a process supports this position. Military leaders should not limit strategic communication means to only those primary capabilities listed above. Strategic communication means should be restricted only by the requirement to achieve the desired information effect on the target audience.

In that light, messages are certainly sent by verbal and visual communications means, but they are also sent by actions. (Note that the definition specifically includes "actions"). In fact, senior officials point out that strategic communication is "80% actions and 20% words."[19] Specifically, how military operations are conducted affects the information environment by impacting perceptions, attitudes and beliefs. As previously noted, DoD has emphasized this fact by referring to strategic communication as the orchestration of actions, images and words.

7. Strategic Communication and IO - A Side by Side Comparison. The current definitions of IO (DoD Dictionary of Terms) and Strategic Communication (DoD Dictionary of Terms) are clear and fairly distinct to the fully engaged information practitioner, but there are nuances that make those distinctions difficult to grasp for others (to include operational commanders) and so clarifying these concepts is well worth considering. Strategic communication is the more broadly overarching concept targeting *key audiences* and focusing on the cognitive dimension of the information environment. IO as an integrating function specifically focuses on *military operations* and so more specifically targets *decision-making of adversaries and potential adversaries*, which may be in the cognitive, informational and/or physical dimensions of the information environment.[20]

	Target	**Effect**	**Dimension**
SC	Key audiences (friendly, neutral, adversarial)	Understand and engage	Cognitive (people)
IO	Adversaries' and potential adversaries' decision-making	Influence, disrupt, corrupt, or usurp	Cognitive, information, physical (people, processes, systems)

Considering the targets and effects described above, it should be clear that both strategic communication and IO can be employed at all levels of warfare (tactical, operational, theater strategic and national strategic). Tactical commanders routinely employ strategic communication in Iraq and Afghanistan today based on their interactions with key audiences in their area of responsibility to a potential strategic end. On the other end of the scale, IO could certainly be employed strategically as part of a shaping Phase 0 operation or a deterrent Phase 1 operation against a potential adversary's decision-making capability.

8. Effectively Integrating Strategic Communication in Military Planning. Remembering that strategic communication is a way to achieve cognitive information effects using any means available takes the mystery out of the concept. Strategic communication simply employs capabilities (limited only to the imagination) to support the achievement of a military objective. Just as a commander integrates air, land and sea capabilities into military planning and execution, he can and should integrate strategic communication capabilities. The planning process is not new. The focus on and understanding of this new concept and its capabilities, however, may be.

First, planners must define the information environment and its physical, informational and cognitive dimensions. How does the target audience receive their information (TV, radio, internet, rumor, religious services, etc.)? How does culture play into the message? Who are the

credible messengers? Next, planners need to consider the desired effect on the cognitive dimension, i.e. the ends or outcome. Does the endstate include changing perceptions, influencing people, gaining acceptance, gaining credibility and trust, gaining support? This will drive how the operation will be conducted where themes and messages are necessary, but not sufficient.

Any military planner will quickly see how this logical thought process fits neatly into the established military decision-making process (or campaign planning process). The information environment is considered in the analysis of the overarching operational environment. The commander's intent establishes an endstate. This must include a statement of the desired information environment endstate. A properly stated information endstate in the commander's intent will guide staffs in the selection of appropriate courses of action and drive subordinate units in the way they conduct operations to achieve that endstate. A selected course of action will then be wargamed using the traditional friendly action, expected enemy reaction, and friendly counteraction methodology. The wargaming process must also occur with an eye toward information effects. This becomes especially important in counterinsurgency operations where the enemy uses information as an asymmetric strategic means and where changing indigenous populations' perceptions can turn them from a neutral position to one in favor of coalition forces. But it also applies across all levels of the spectrum of conflict in an environment where military operations will likely be covered in real time by both mainstream and "new" media sources.

9. Conclusion. Strategic communication is simply a way to affect perceptions, attitudes and behaviors of key audiences in support of objectives. Certainly communications means are very important in ultimately achieving those desired information effects. But *how* military operations are conducted or policy is implemented is also a key component of strategic communication, since actions send very loud and clear messages. Effective strategic communication requires an organizational culture attuned to the information environment and a recognition that strategic communication, as a way to achieve information effects, consists of many capabilities (means) that are an integral part of the leader's arsenal.

Dennis M. Murphy
Professor of Information Operations and Information in Warfare
U.S. Army War College

Endnotes

---

[1] Ronald Reagan, *National Security Decision Directive 130* (Washington, DC: The White House, 6 March 1984) Available from http://www.fas.org/irp/offdocs/nsdd/nsdd-130.htm. Internet. Accessed 25 October 2011.

[2] NATO doctrine (AJP01) cites the "essential trinity of diplomacy, economic and military power, each of which equates to an instrument of national power. These are fed in turn by the instrument of information, which is the fourth corner of the instruments of national power." (Allied Joint Doctrine, December, 2010).

[3] Robert E. Neilson and Daniel T. Kuehl, "Evolutionary Change in Revolutionary Times: A Case for a New National Security Education Program," *National Security Strategy Quarterly* (Autumn 1999): 40.

[4] Barack Obama, National Framework for Strategic Communication (Washington, DC: The White House, March 2010) Available from http://www.carlisle.army.mil/dime/documents/National%20Strategy%20for%20Strategic%20Communication.pdf. Internet. Accessed 25 October 2011.

[5] U.S. Department of Defense, *DOD Dictionary*, http://www.dtic.mil/doctrine/jel/doddict/data/p/11548.html (accessed 25 October 2011).

[6] *Broadcasting Board of Governors Home Page*, http://www.bbg.gov/, (accessed 25 October 2011).

[7] John S.D. Eisenhower, *Agent of Destiny: The Life and Times of General Winfield Scott* (New York: The Free Press, 1997) 245-6.

[8] The Smith-Mundt Act is still in effect to include the requirement not to "target" U.S. audiences (with any number of interpretations on what U.S. government organizations it pertains to). The current information environment with ubiquitous, world-wide digital outlets, satellite communications and real-time reporting makes it difficult to target foreign audiences without exposing U.S. audiences to the message, however…a fact not envisioned in 1948 when the act became effective.

[9] David E. Kaplan "Hearts, Minds, and Dollars." *U.S. News and World Report*, April 25, 2005, 25, 27.

[10] "Senior Officials: Under Secretary for Public Diplomacy and Public Affairs," linked from *U.S. Department of State Homepage* http://www.state.gov/misc/19232.htm (accessed 25 October 2011).

[11] Executive Order 13584, *Federal Register***,** Vol. 76, No. 179, September 15, 2011. http://www.carlisle.army.mil/dime/documents/Executive%20Order%2013584.pdf (accessed 25 October 2011)

[12] QDR Execution Roadmap for Strategic Communication, 3.

[13] Robert Gates, "Department of Defense Report on Strategic Communication," Washington, DC: December 2009, 1.

[14] U.S. Principal Deputy Assistant Secretary of Defense for Public Affairs Robert T. Hastings, "Principles of Strategic Communication," memorandum for Secretaries of the Military Departments, et. al., Washington, DC, August 15, 2008.

[15] U.S. Joint Forces Command, *Commander's Handbook for Strategic Communication and Communication Strategy* (Norfolk, VA: Joint Warfighting Center, June 24, 2010), III-6. This manual indicates that "eight combatant commands are either employing or transitioning to this model."

[16] QDR Execution Roadmap for Strategic Communication, 2.

[17] Chairman of the Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13, (Washington, DC: Joint Chiefs of Staff, February 13, 2006), I-13.

[18] Harry R. Yarger, "Toward a Theory of Strategy: Art Lykke and the Army War College Strategy Model," *U.S. Army War College Guide to National Strategy and Policy* (June 2006): 107.

[19] The author has attended numerous briefings by the Office of the Assistant Secretary of Defense (Public Affairs) where this has been stated.

[20] The definition of Information Operations recently changed. Notably, the core capabilities, formally included in the definition, fell out.

This Page Intentionally Blank

Cyberspace and Cyberspace Operations

This section addresses the evolving nature of cyberspace, specifically focusing on its influence on, and implications for, all instruments of national power. It also addresses the need for continued development of theory, organization, and mission for cyberspace operations related to national security. The section was added as part of the AY10 edition, and each subsequent version includes significant new material based on policy and strategy changes during the year.

1. Introduction.

a. Definition. DoD defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers,"[1] and it can be argued this should also include their operators. In a broader sense, cyberspace is "a new strategic common, analogous to the sea as an international domain of trade and communication."[2]

b. History--Enduring vice Modern Cyberspace. In a simple form, the cyberspace process consists of elements within the three dimensions of the information environment – cognitive, information, and physical (sometimes called cognition, content, and connectivity).[3] For example, someone generates a thought (cognitive); which they enter into a communication device (physical) where it becomes a systematic representation of data (information), possibly represented digitally using electromagnetic means. Next, the data travels through physical lines of communication (e.g., telephone, cable, fiber optic, radio, etc) where it exits through a communication device for cognitive uses, or perhaps to perform kinetic operations (e.g., turn on a light, open a valve, etc). Cyberspace then is the total of all elements required for cyberspace processes to occur. The fundamental structure of the cyberspace process is enduring; but the configuration of cyberspace itself transforms when specific elements of the basic process transform. Consider the development of the telegraph as an early example of the cyberspace process evolution. In the mid-twentieth century, the process was transformed with electronic transistor-based data processing devices. One could argue that modern cyberspace emerged due to the convergence of three events--the introduction of the personal computer (circa 1975), the Internet (circa 1982), and the worldwide web protocol (circa 1989).[4]

c. Cyberspace as a Global Common. When considered as a strategic commons (or global commons), cyberspace has at least five unique characteristics. First, the cost of entry and access to cyberspace is low—basically the cost of a laptop and Internet café fee. Second, cyberspace offers a degree of anonymity that challenges efforts to detect, track, and target a specific user who desires to hide in the common. Third, cyberspace provides the ability to initiate a variety of physical effects across vast distances at almost instantaneous speeds. Fourth, cyberspace is an ever-growing common mostly owned and operated by private individuals and corporations; it expands with every new computer server or Internet-capable mobile device. Finally, cyberspace does not have traditional dimensions of height, depth,

and length, but it does have unique metrics that can be used to map its boundaries and operations.

2. Dynamic Nature of Contemporary Cyberspace Evolution.

a. Connectivity. Innovations in computer technology have greatly enhanced the ability of the average citizen to operate freely in cyberspace. Data processing speeds and digital storage media continue to grow exponentially with competitive markets that drive sales prices down. In early 2009, China first surpassed the U.S. in number of Internet users (253 million vice 220 million); the gap has grown significantly, and in June 2011 China reached 485 million users compared to 245 million in the U.S.. Together, they account for over 34 percent of the over 2.1 billion users worldwide; the top 20 countries account for over 75 percent of all Internet users.[5] With 216 countries or territories having Internet access, 101 of which have at least one million users,[6] it is becoming difficult to find any place in the world not affected by cyberspace.

It is not surprising that industry and government leverage the ability of cyberspace-based remote access to control infrastructure. Usually called Supervisory Control and Data Acquisition (SCADA) systems, these control processes increase effectiveness and efficiency for systems such as electric power, oil, gas, transportation, and telecommunications.[7] Often, older SCADA devices were designed without regard for security, and most new SCADA systems use the Internet to pass control information. As the population of Internet users pushes well beyond two billion, it is wise to pursue better security for any physical systems accessible via cyberspace.

b. Threats. In general, attacks in cyberspace involve activities that disrupt, deny, degrade, or destroy information. Attacks may be overt or covert with kinetic or non-kinetic effects. The damage inflicted varies greatly--from defaced websites, to multi-million-dollar financial losses, and even to actual physical damage to equipment connected to cyberspace. Perpetrators differ in attitudes and actions regarding ideology (e.g., political or religious), monetary gain, attribution, knowledge sharing, and destruction of societal structures. All but the most extreme individuals (e.g., anarchists) have a vested interest in the preserving cyberspace infrastructure—the domain from which they derive power. Cyberspace wrongdoers may interact for mutual benefit and may exploit law-abiding operators. There are documented cases where cyber-terrorists employed cyber-criminals to steal credit card information and support drug traffickers, all toward the goal of funding terrorist operations. Another lucrative business is the marketing of "botnets," virtual armies of compromised computers that can be controlled remotely over the Internet by a "botmaster". Botnets may exploit hundreds of thousands of computers, usually without the owners' knowledge.[8] An adversary with such capability could achieve swarming attacks and defenses—in cyberspace as well as other strategic commons—that challenge the "traditional mass- and maneuver-oriented approaches to conflict."[9]

What is less clear is how state and nonstate actors are using cyberspace to pursue strategic goals. For example, the Conficker botnet was first launched in 2008 and morphed into at least four variants in 2009; its design was so sophisticated that analysts conclude it is either backed by organized crime or a nation-state. Industry estimates claim as many as 12 million computers may have been infected, of which several million remain as a stable botnet with an unrevealed objective.[10] Another high-profile enigma is Stuxnet, a worm designed with the popularly reported purpose of attacking the control systems of Iran's nuclear program.[11] According to the Symantec Corporation, Stuxnet first appeared in June 2009, and it targeted five Internet domains in three waves of attack. Often called a precision cyberspace weapon, by September 2010 Stuxnet actually had infected over 100,000 systems in more than 25

countries indicating that it had significant "collateral damage" due to its propagation method.[12]

Among these potential state adversaries, China's emerging capabilities in cyberspace reflect an asymmetrical approach consistent with the classical Chinese strategic thinkers.[13] In 2009, a Report to Congress stated that the People's Liberation Army (PLA) "views computer network warfare as both a key enabler of modern warfare and a critical new spectrum of conflict in its own right." The guiding PLA operational concept called "Integrated Network Electronic Warfare" advocates employment of traditional electronic warfare elements (e.g., jammers) coordinated with computer network attack. Employment of the cyber forces may use small groups with specialized skills and tasks, such as reconnaissance, breach, and collection teams. Attacks attributed to China include exfiltration of "several terabytes of data related to design and electronics systems of the F-35 Lightning II," an advanced U.S. multiservice fighter plane, which will also serve in many allied countries.[14]

The November 2010 Report to Congress concluded that China Internet users continue to hack into American networks as well as those of foreign entities and governments. Recent high-profile, China-based computer exploitations continue to suggest some level of state support. The report also identifies three emerging trends of concern: penetrators' methods use more sophisticated techniques; leverage social networking tools; and exploit malicious software tied to the criminal underground—"both to distance themselves from attribution and to strategically cultivate a climate of uncertainty." Several incidents in early 2010 demonstrate that, regardless of whether Chinese actors actually intended to manipulate U.S. and other foreign Internet traffic, China's Internet engineers have the capability to do so. For example, in April 2010 a large number of routing paths to various Internet Protocol addresses were redirected through networks in China for 17 minutes, giving the network server operators the ability to read, delete, or edit e-mail and other information sent along those paths by U.S. government, military, and business sites. This and other incidents raise questions about whether China might seek to leverage these abilities intentionally to assert some level of control over the Internet, even if only for a brief period.[15]

3. Cyberspace and Instruments of National Power.

a. Diplomatic. How should countries interact in cyberspace? Does this new common require entirely new standards of conduct? As independent governments, countries have an international obligation to act in good faith and settle disputes with other states by peaceful means. If conflict should occur, the right of using proportional force in self-defense is a cornerstone of international security. Legal experts argue that "it now seems almost universally accepted that a considerable body of international law does indeed apply to the use of force by states in CyberSpace."[16] However, the widely distributed nature of cyberspace does not necessarily recognize national boundaries, and new provisions to address this reality seem prudent. A successful example is the Council of Europe Convention on Cybercrime, a formal agreement among countries "to better combat cybercrime by harmonizing national laws, improving investigative abilities, and boosting international cooperation." The convention, which began in 1997, was opened for signature on 23 November 2001 and has been ratified by at least 32 countries. Its provisions include definition of criminal offenses in four categories (fraud and forgery, child pornography, copyright infringement, and security breaches) as well as methods to address these crimes.[17] The U.S. Department of Justice has arrested and convicted domestic and international individuals and small groups committing cyberspace-related crimes since 1998. The department determines whether the crime targeted a private individual or corporation, or a government agency as well as whether the crime posed a threat to public health or safety (i.e., power grids, air traffic control, etc.).[18] The attackers include citizens from China,

Russia, Estonia, Moldova, Kazakhstan, Israel, and the United Kingdom. In some cases, extradition requests were pursued per the Convention on Cybercrime.[19]

A July 2010 report by the Government Accountability Office identifies at least 15 major existing cyberspace governance bodies that require State Department involvement.[20] In December 2010, Secretary of State Hillary Clinton released the first *Quadrennial Diplomacy and Development Review (QDDR)*, which among other global threats, addressed "the cybersecurity risk that comes from our dependence on technology and online networks. The same technologies that promote global prosperity and the free flow of information also create new vulnerabilities." This dual-nature of cyberspace efforts--opportunity and vulnerability—is a consistent thread throughout the report. It goes on to state, "We need to defend our information networks and critical infrastructure against attacks from cyberspace, and protect our government institutions and businesses against cybercrime and espionage." The report revealed the creation of a State Department Coordinator for Cyber Issues whose duties include leading the Department's diplomatic engagement on cyber issues with international Allies and partners.[21]

In May 2011, Secretary Clinton released the *International Strategy for Cyberspace* with the goal to promote a cyberspace environment that is "open, interoperable, secure, and reliable" based on "norms of responsible behavior." The document is divided into three approaches for the future—diplomacy, defense, and development—and supported by seven policy priorities. The strategy promulgated the need for coordinated activities that address all instruments of national power—diplomatic, information, military, and economic. The strategy reiterated the need to develop and maintain partnerships with other countries as well as private sector, noting that "no single institution, document, arrangement, or instrument could suffice in addressing the needs of our networked world." It also includes an explicit call to "actively engage the developing world" in terms of support for universal freedoms as well as access to technological advancements.[22]

b. Information. How can information be stored safely in cyberspace? The U.S. government views information technology (IT) as one sector of the nation's critical infrastructure and has tasked the Department of Homeland Security (DHS) to direct its protection. In turn, DHS created a National Cyber Security Division in June 2003 to serve as a focal point for cybersecurity issues. Working to avoid information sharing failures that contributed to the September 2001 terrorist attacks, DHS conducted 16 major cyber exercises between 2004 and 2008, which included participants from federal, state, and local governments as well as ones from private industry, academe, and foreign governments.[23]

DHS continues to improve its efforts toward national cybersecurity. In October 2009, DHS Secretary Napolitano opened the new National Cybersecurity and Communications Integration Center (NCCIC), a 24-hour center to identify and mitigate risks to critical U.S. cyberspace infrastructure.[24] The February 2010 Quadrennial Homeland Security Review (QHSR) Report identified "Safeguarding and Securing Cyberspace" as one of its five missions, with goals to "create a safe, secure, and resilient cyber environment" and to "promote cybersecurity knowledge and innovation."[25] To facilitate better coordination, DHS released an interim version of a new National Cyber Incident Response Plan in September 2010, which includes appendices that define roles and responsibilities for several departments (e.g., defense, state, justice); for state, local, tribal, and territorial authorities; and for the private sector.[26] The NCCIC and the new response plan were tested later that month in exercise Cyber Storm III, which included participation from 12 international partners and 60 private sector companies.[27] The July 2011 exercise final report identifies five key findings: (1) the NCIRP is a good foundation that needs further maturing; (2) public-private interaction is improving but still lacks sufficient shared situational awareness; (3) a

cyber common operating picture (COP) across the community is a critical requirement; (4) the National Cyber Risk Alert Level (NCARL) intended to inform preparedness and decision-making requires further refinement; and (5) the government, private, and public sectors rely on public and strategic communication to manage network threats.[28]

At the Executive level, President Bush signed Homeland Security Presidential Directive 23 in January 2008, better known as the Comprehensive National Cybersecurity Initiative (CNCI). Originally a classified document, three of the CNCI major "public" priorities support the access points, data traffic, and security protocol for information traversing U.S. government agencies' computer networks.[29] On 29 May 2009, President Obama announced the completion of a "60-day, comprehensive, 'clean slate' review to assess U.S. policies and structure for cybersecurity." In December 2009, Howard Schmidt was appointed as the first White House Cybersecurity Coordinator, and a member of both the National Security Staff and the National Economic Council."[30] Several months later, Mr. Schmidt announced the revised classification of the CNCI to include an unclassified description of 12 initiatives for anyone to download.[31]

In May 2010, the new National Security Strategy included a subsection on "Secure Cyberspace" that identified "our digital infrastructure" as "a strategic national asset, and protecting it—while safeguarding privacy and civil liberties—is a national security priority." Further, it emphasized investing in people and technology along with strengthening partnerships—government, private, and international—as means by which "we will deter, prevent, detect, defend against, and quickly recover from cyber intrusions and attacks."[32] In July 2010, Mr. Schmidt released a Progress Report on Cybersecurity that provided examples of work accomplished toward the CNCI and Cyberspace Policy Review actions, such as the deployment of EINSTEIN network intrusion detection technology to 12 of 19 federal agencies.[33] In April 2011, the *National Strategy for Trusted Identities in Cyberspace* was released with its stated vision of "Individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation." The realization of this vision is the user-centric "Identity Ecosystem" described in the strategy that is "designed to securely support transactions that range from anonymous to fully-authenticated and from low- to high-value."[34] In May 2011, Mr. Schmidt announced that the 10 near-term actions of the Cyber Policy Review were complete, although a dedicated document for the Cyber Research and Development Framework has still not been released.[35]

c. Economic. The costs to industry of cybersecurity breaches are high. The 2010 *Annual Threat Assessment of the Intelligence Community* estimates total cyber-related business losses in 2008 to be 42 billion dollars for the U.S. and 140 billion dollars globally, as well as possibly one trillion dollars worth of intellectual property lost globally.[36] Determining when an attack occurs in business is difficult, and it is challenging to measure the cost of attacks. However, the 2011 *World Threat Assessment* estimates that the volume of malicious software ("malware") on American networks has more than tripled from 2009, and that two-thirds of U.S. firms report cybersecurity incidents.[37] The Commerce Department launched the Internet Policy Task Force in April 2010 to identify and address the Internet's most pressing policy issues and to recommend new policies. The Task Force was directed to look at establishing practices, norms and ground rules that promote innovative uses of information in four key areas where the Internet must address significant challenges: enhancing Internet privacy; improving cybersecurity; protecting intellectual property and encouraging the global free flow of information. In June 2011, Commerce Secretary Gary Locke released a "green paper" status of the task force. The report notes that industry estimates that the Internet "global network helps to facilitate $10 trillion in online transactions

every single year"—influencing over 13 percent of the total estimated world value ($74.5 trillion)—without a doubt, the Internet is a player in the world economy. Unfortunately, the report is a work in progress, with no details for when policy and guidance will be formally developed, let alone implemented.[38]

The trends of economic cybercrime continue with increased sophistication of targeting and extraction techniques employed by thieves. Deputy Secretary of Defense William Lynn put this perspective by writing "every year, an amount of intellectual property many times larger than all the intellectual property contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government agencies." Such sustained losses erode the U.S. ability to compete in the global economy.[39] Fortunately, the FBI is working with international partners to dismantle cyber criminal organizations. For example, they led the take-down of a Russian-led organization, which penetrated over 300 financial institutions worldwide (including the Royal Bank of Scotland), where the "actors coordinated the withdrawal of nearly $10 million in less than 24 hours from more than 2,100 ATMs in 280 cities around the world."[40] In April 2011, the FBI shut down the Coreflood botnet, which had stolen 190 gigabits of banking passwords and other sensitive data from over 413,000 infected systems.[41]

d. Military. How are traditional military organizations embracing operations in cyberspace? In his January 2009 testimony before Congress, Secretary of Defense Robert Gates acknowledged the extent of the threat: "With cheap technology and minimal investment, current and potential adversaries operating in cyberspace can inflict serious damage to DoD's vast information grid—a system that encompasses more than 15,000 local, regional, and wide-area networks, and approximately 7 million IT devices."[42] The February 2010 *Quadrennial Defense Review (QDR) Report* includes "operate effectively in cyberspace" as one of the six key DoD missions. The report listed four steps DoD is taking to strengthen its capabilities in cyberspace: "Develop a comprehensive approach to DoD operations in cyberspace; Develop greater cyberspace expertise and awareness; Centralize command of cyberspace operations; Enhance partnerships with other agencies and governments."[43]

Recent events provide insight regarding the approach offered in the QDR. In April 2007, the Estonian governmental, commercial and private organizations endured three weeks of cyber attacks. Responding to an historic request by a member state of the North Atlantic Treaty Organization (NATO) in defense of its digital assets, the U.S. sent computer security experts to Estonia to help with recovery efforts.[44] The aftermath of this attack included the creation of two new cybersecurity organizations. At the operational level, the Cyber Defence Management Authority (CDMA) was established in Brussels, Belgium.[45] At the strategic level, the Cooperative Cyber Defence Center of Excellence (CCD CoE) was established at Tallinn, Estonia "to enhance the cooperative cyber defence capability of NATO."[46] In August 2008, the movement of Russian tanks into Georgia coincided with distributed denial of service attacks on Georgian websites. While there may be no conclusive evidence proving the cyber attacks were carried out or sanctioned by the Russian government, their timing with the conventional attacks cannot be ignored.[47] Also in 2008, DoD suffered a compromise of classified military computers when a malicious code on a flash drive in U.S. Central Command created "what amounted to a digital beachhead, from which data could be transferred to servers under foreign control." The U.S. response to counter the attack, named Operation Buckshot Yankee, "marked a turning point in U.S. cyberdefense strategy."[48] More recently, in October 2011, there were press reports of computer viruses "potentially threatening the reliability of the drones during combat as well as operational security before missions."[49] Indeed, the U.S. Air Force confirmed that "malware was detected on a stand-alone mission support network" but further clarified that "the detected

and quarantined virus posed no threat to our operational mission and that control of our remotely piloted aircraft was never in question."[50]

On 23 June 2009, Secretary Gates directed the development of a new national strategy for cybersecurity as well as the establishment of U.S. Cyber Command (USCYBERCOM) as a subordinate unified command under U.S. Strategic Command (USSTRATCOM). He specified a structure, which includes Service components as well as support from the Defense Information Systems Agency (DISA). Also, it has Title 10 and Title 50 responsibilities using a dual-hat structure with the commander, USCYBERCOM also serving as director, National Security Agency (NSA). The former Joint Task Force-Global Network Operations (JTF-GNO) and Joint Functional Component Commander-Network Warfare (JFCC-NW) were disestablished and their missions subsumed into USCYBERCOM.[51] On 31 October 2010, USCYBERCOM achieved Full Operational Capability, with its mission to direct operations and defense of DoD networks, conduct full-spectrum military cyberspace operations, and ensure U.S. and Allied freedom of action in cyberspace and deny the same to adversaries.[52]

In July 2011, the *DoD Strategy for Operating in Cyberspace* was publically released as "the first DoD unified strategy for cyberspace and officially encapsulates a new way forward for DoD's military, intelligence and business operations."[53] The strategy is built upon five strategic initiatives: (1) *Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential.* (2) *Employ new defense operating concepts to protect DoD networks and systems.* (3) *Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy.* (4) *Build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity.* (5) *Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.*[54] These initiatives mesh well with the tenets of the June 2010 NATO Policy on Cyber Defence, which "provides a solid foundation from which Allies can take work forward on cyber security" emphasizing prevention, resilience, and non-duplication. The Cyber Defence Programme includes a NATO Computer Incident Response Capability (NCIRC) planned to be fully operational in 2012.[55]

In his testimony before Congress in June 2011, Secretary of Defense nominee Leon Panetta reiterated the importance of DoD support of national security efforts in cyberspace: "I have often said that there is a strong likelihood that the next Pearl Harbor that we confront could very well be a cyber attack that cripples our power systems, our grid, our security systems, our financial systems, our governmental systems".[56]

4. Cyberspace Operations Issues.[57]

a. Cyberspace Operations in the Joint Operating Environment (JOE). The 2010 JOE provides an intellectual foundation to build concepts for future force development, which includes the continuing trend of cyber-related technologies changing how military operations are conducted at the tactical, operational, and strategic levels. The January 2009 *Capstone Concept for Joint Operations* (CCJO) further elaborates on the changing nature of cyberspace in joint operations, providing broad precepts and assertions to help guide the development and employment of future joint forces. Figure 1 provides a summary of many of the key concepts of cyberspace operations espoused within the JOE and CCJO. One overarching concept is the envisioned emergence of cyberspace as a global common that demands freedom of maneuver at the strategic level as well as localized domain superiority as a requisite for successful future expeditionary operations. Also, there is a consistent expectation that future conflict will not only include cyberspace operations, but also that the

cyberspace common itself may become a main front in both irregular and traditional conflict.[58]

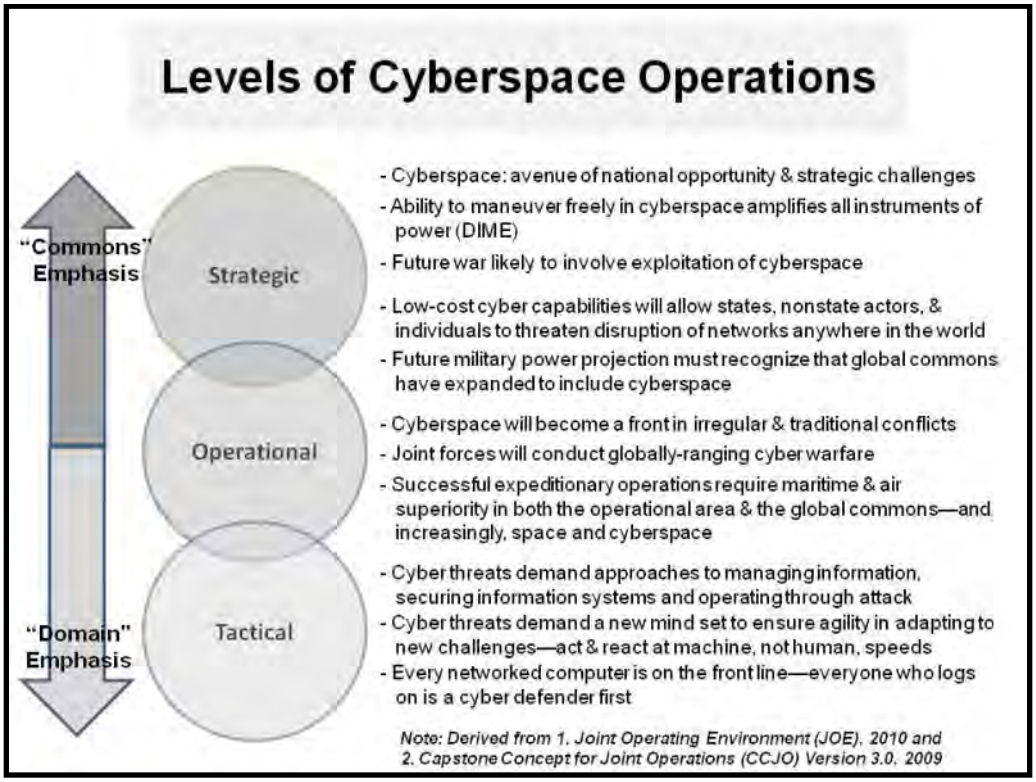


Figure 1. Levels of Cyberspace Operations

b. War in Cyberspace. As cyberspace becomes a contested global common, will this require new definitions for war and deterrence? No consensus answer to this question has emerged yet. There is no internationally accepted definition of when hostile actions in cyberspace are recognized as attacks, let alone acts of war. However, scholars are making progress in this area, such as the application of an analytical framework developed by Professor Michael Schmitt that attempts to determine if a cyber attack equates to the use of force in accepted terms of the United Nations (UN). The Schmitt Analysis considers the intensity of damage in each of seven areas (severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility) to provide a composite assessment of the effects of the cyber attack (see Figure 2).[59]

A 2009 study by the National Research Council of the National Academies recommends a basic framework for the legal analysis where potential cyberattack events "should be judged primarily by the effects of an action rather than its modality." Further, it addresses implications of such a framework using Article 51 of the UN Charter for attacks prior to acknowledged armed conflict and the standard law of armed conflict (LOAC) criteria for acknowledged conflict. Current U.S. military doctrine is developing along philosophical lines that distinguish between the warfighter (Title 10) role of cyberattack and the intelligence (Title 50) role of cyberexpolitation. Terminology to describe cyberspace operations in general, as well as specific concepts of attack, defense, and the electromagnetic spectrum, still varies among Services.[60] Completion of the new Joint Publication 3-12, "Cyberspace Operations" and USSTRATCOM's Cyberspace Joint Operating Concept should enhance unity of effort.[61]

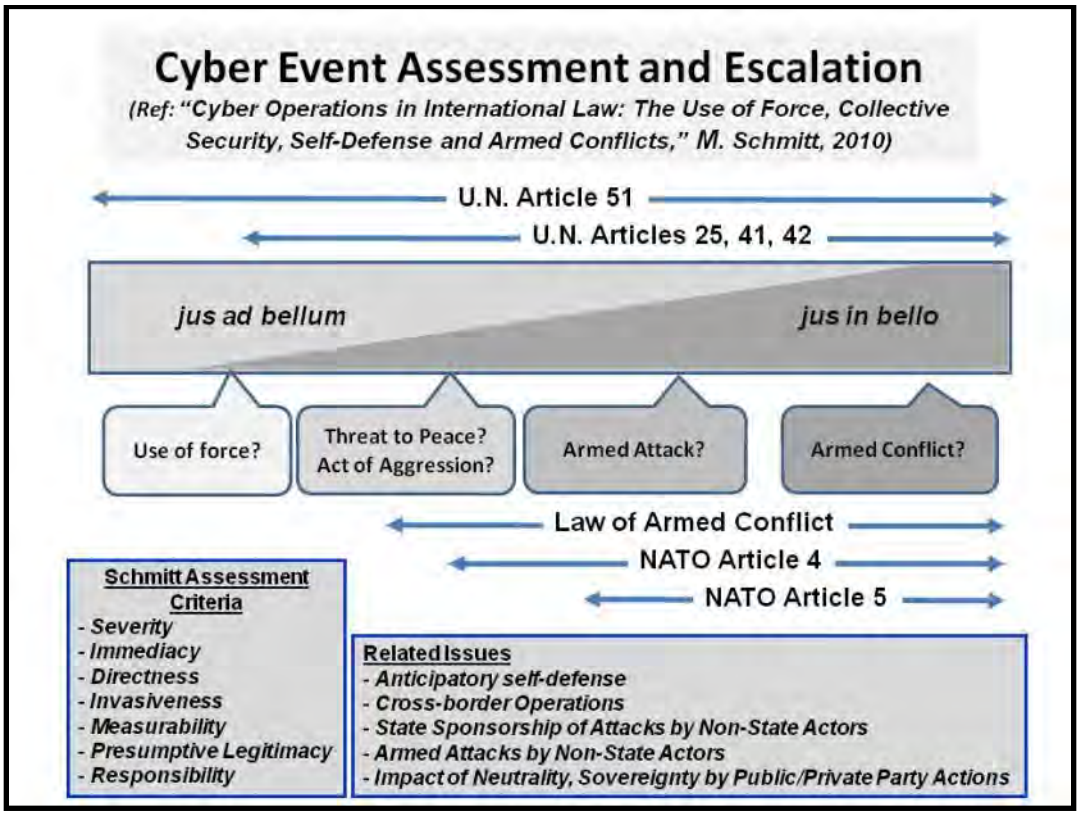


Figure 2. Cyber Event Assessment and Escalation Continuum Factors

c. Cyberspace Theory Development. In general, theory provides the overarching abstract thought and philosophical foundation necessary to analyze a given concept with appropriate rigor. Given the models of cyberspace as both an operational domain and a global common, what is the best approach to develop its theory of operation? A valuable analogy is that of traditional (i.e., Mahan) naval theory, part of which involves the difference between naval operations in the littoral area—the "brown water"—versus those in the broad ocean area—the "blue water." Simply put, when one connects the major ports in the "brown water" to other ports in the world, "sea lines of communication" emerge that have strategic importance based on many factors including geography and volume of traffic.[62] Similarly, cyberspace can be mapped using techniques that clearly show its "cyber lines of communication" and critical nodes with tactical, operational, and strategic implications for their control, perhaps even choke points—the "blue water cyberspace" equivalent of the Straits of Malacca.[63]

The security of these critical nodes—some may be physical, others informational—should interest anyone attempting to protect or exploit cyberspace. Thus, it may be prudent to "evolve from a perimeter-defense strategy to a defense-in-depth strategy" where we "provide higher levels of security to more valuable, mission-critical resources" and consider the possibility that "we may have to sacrifice less critical assets or even networks during an attack."[64] Indeed, the new DoD Strategy for Operating in Cyberspace has "employ new defense operating concepts to protect DoD networks and systems" as one of its five strategic initiatives. A more holistic approach to cyberspace defense has been offered by DHS based on the concept of a "cyber ecosystem" similar to a healthy and resilient human body, where participants and devices in cyberspace work together to "prevent cyber attacks,

limit the spread of attacks across participating devices, minimize the consequences of attacks, and recover to a trusted state."[65]

d. Deterrence in Cyberspace. The CNCI establishes an initiative to "define and develop enduring deterrence strategies and programs…aimed at building an approach to cyber defense strategy that deters interference and attack in cyberspace." Our allies also recognize the rising danger of cyber attacks and the November 2010 Lisbon summit's new NATO Strategic Concept calls for a "full range of capabilities necessary to deter and defend against any threat" among which is the requirement to "develop further our ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities."[66] Developing cyberspace deterrence is a complex and challenging task still in its infancy. Traditional Cold War deterrence experience should be studied, but its model of assured retaliation may have limited application in cyberspace, given the capabilities of nonstate actors as well as the possibility of cyberattacks originating from co-opted servers in neutral countries.[67]

The U.S. *International Strategy for Cyberspace* includes the existing principle that "consistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace." The section on defense of cyberspace does not mince words, stating "when warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country." Further, the U.S. will "reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests." These words send a serious deterrent message to potential adversaries without limiting the type of U.S. response.[68]

e. The Future of Cyberspace. Three initiatives in the CNCI call for expanded and integrated approaches for the U.S. future in cyberspace—coordinating research and development efforts; expanding cyber education; and developing enduring "leap ahead" technologies. The CNCI assesses ongoing efforts as good, but limited in focus and in need of unity of effort. An example of innovation is the National Cyber Range program developed by the Defense Advanced Research Projects Agency, basically a model of the Internet that will allow the testing of cyberdefense capabilities before fielding them.[69] Even these efforts only scratch the technological surface of the complexities of future cyberspace organizations.

5. Conclusion.

Cyberspace is a modern embodiment of an enduring process, accelerated by technology, that combines cognitive, physical, and information elements. Cyberspace has significant influences on, and implications for, all instruments of national power. The national security aspects of cyberspace are still evolving and the release of national strategies for diplomatic, informational, and military instruments of U.S. power has provided an initial foundation for unity of effort. DoD continues to work toward a more holistic security approach organized within a new subunified command as part of a greater team of government, private, and international partners. However, much work remains in the practical definitions of war and deterrence in cyberspace as well as the development of fundamental cyberspace theory. Strategic leaders should study and embrace implications of the growing roles of cyberspace operations in future conflict. Such operations currently fulfill supporting roles, but in time, may become a main front of war itself.

Jeffrey L. Caton
Associate Professor of Cyberspace Operations
U.S. Army War College

Endnotes

[1] U.S. Deputy Secretary of Defense Gordon England, "The Definition of 'Cyberspace'," memorandum for Secretaries of the Military Departments, Washington, DC, May 12, 2008.

[2] Arthur K. Cebrowski, "Transformation and the Changing Character of War?" *Transformation Trends*, June 17, 2004, http://www.afei.org/transformation (accessed 27 March 2009).

[3] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," Chapter 2 in *Cyberpower and National Security* (Washington DC: National Defense University Press and Potomac Books, 2009), 24-42.

[4] Jeffrey L. Caton, "What do Senior Leaders Need to Know about Cyberspace," in *Crosscutting Issues in International Transformation: Interactions and Innovations among People, Organizations, Processes, and Technology,* ed. Derrick Neal et al (Washington DC: National Defense University, 2009).

[5] *Top 20 Countries with the Highest Number of Internet Users*, Internet World Stats. http://www.internetworldstats.com (accessed 31 March 2009 and 24 October 2011). As of 30 June 2011, the top 20 countries in order are: China, United States, India, Japan, Brazil, Germany, Russia, United Kingdom, France, Nigeria, Indonesia, Korea, Iran, Turkey, Mexico, Italy, Philippines, Spain, Vietnam, and Argentina.

[6] "Country Comparisons—Internet Users," *The World Factbook* (Washington, DC: Central Intelligence Agency, 2009), https://www.cia.gov/library/publications (accessed 24 October 2011).

[7] Samuel G. Varnado, "SCADA and the Terrorist Threat: Protecting the Nation's Critical Control Systems," (Washington, DC: U.S. House of Representatives, October18, 2005). See also "Experiment Showed Grid Vulnerability to Cyber Attack – Flaws Fixed," *Energy Assurance Daily* (Washington, DC: U.S. Department of Energy, September 27, 2007). The DoE reported on recommended changes to power generation facilities resulting from a DHS experiment in March 2007. The test demonstrated the ability to cause catastrophic physical damage to an industrial turbine via commands sent through its SCADA system.

[8] Clay Wilson, Botnets, *Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, CRS Report for Congress RL-32114 (Washington, DC: Congressional Research Service, January 29, 2008).

[9] John Arquilla and David Ronfeldt, "The Advent of Netwar (Revisited)," in *Networks and Netwars* (Santa Monica: RAND, 2001), 12.

[10] Mark Bowden, "The Enemy Within," *The Atlantic*, June 2010 and *Worm: The First Digital World War* (New York: Atlantic Monthly Press, 2011).

[11] Gross, Michael Joseph. "Stuxnet Worm: A Declaration of Cyber-War," *Vanity Fair*, April 2011.

[12] Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxnet Dossier*, Version 1.4 (Cupertino CA: Symantec Corporation, February 2011).

[13] Timothy L. Thomas, *Decoding the Virtual Dragon: Critical Evolutions in the Science and Philosophy of China's Information Operations and Military Strategy* (Fort Leavenworth, KS: Foreign Military Studies Office, 2007).

[14] *2009 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington DC: U.S. Government Printing Office, November 2009), 167-180.

[15] *2010 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington DC: U.S. Government Printing Office, November 2010).

[16] Walter G. Sharp, *CyberSpace and the Use of Force* (Falls Church: Aegis Research, 1999).

[17] Kristin Archick, *Cybercrime: The Council of Europe Convention*, CRS Report for Congress RS21208 (Washington, DC: Congressional Research Service, September 28, 2006). "Convention on Cybercrime Status of Signatures and Ratifications" (Council of Europe, October 24, 2009) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (accessed October 24, 2011). Note that in addition to the 32 countries that have ratified the convention, 15 additional countries are non-ratified signatories.

[18] Department of Justice, *Computer Crime Cases* (Washington: Department of Justice) http://www.cybercrime.gov/cccases.html (accessed 24 October 2011). The U.S. Department of Justice claiming jurisdiction for cyberspace crimes with physical impacts on U.S. individuals and organizations is not the same as suggesting there is a "U.S. cyberspace boundary."

[19] Department of Justice, U.S. Attorney Sally Quillian Yates, Northern District of Georgia, *International Hacker Arraigned after Extradition: Elaborate Scheme Stole over $9.4 Million from Credit Card processor* (Washington, DC: Department of Justice, 2009) http://www.cybercrime.gov/tsurikovArraig.pdf (accessed 24 October 2011).

[20] U.S. Government Accountability Office, *United States Faces Challenges in Addressing Global Cybersecurity and Governance* (GAO 10-606), (Washington, DC: GAO Office, July 2010).

[21] U.S. Secretary of State Hillary Rodham Clinton, *Leading Through Civilian Power: The First Quadrennial Diplomacy and Development Review* (Washington, DC: U.S. Department of State, December 2010).

[22] Barack Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, May 2011).

[23] U.S. Government Accountability Office, *Critical Infrastructure Protection: DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise* (GAO-08-825), (Washington, DC: GAO Office, September 2008).

[24] Department of Homeland Security, *Secretary Napolitano Opens New National Cybersecurity and Communications Integration Center*, Press Release (Washington DC: DHS, October 30, 2009).

[25] U.S. Secretary of Homeland Security Janet Napolitano, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland*, (Washington, DC: U.S. Department of Homeland Security, February 2010): 54-58, 77.

[26] U.S. Department of Homeland Security, *National Cyber Incident Response Plan, Interim Version* (Washington, DC: Department of Homeland Security, September 2010).

[27] U.S. Department of Homeland Security, *Fact Sheet: Cyber Storm III* (Washington, DC: Department of Homeland Security).

[28] Department of Homeland Security Office of Cybersecurity and Communications, National Cyber Security Division, *Cyber Storm III Final Report*, (Washington DC: DHS, July 2011).

[29] Brian Lake, "CyberThreats: A Cultural Change of Combating Threats," *Homeland Defense Journal* 6 no. 7 (December 2008): 14-16.

[30] Macon Phillips, "Introducing the New Cybersecurity Coordinator," (Washington DC: The White House Blog, December 22, 2009).

[31] *The Comprehensive National Cybersecurity Initiative (CNCI),* (Washington DC, The White House, March 2, 2010.

[32] Barack Obama, *National Security Strategy* (Washington DC, The White House, May 2010): 27-28.

[33] Howard Schmidt, *Progress Report on Cybersecurity* (Washington DC, The White House Blog, July 14, 2010). Also see GAO report: *Executive Branch is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership is Needed*, Report GAO-11-24 (Washington DC, U.S. Government Accountability Office, October 2010).

[34] Barack Obama, *National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security and Privacy*, (Washington DC: The White House, April 2011).

[35] *Fact Sheet: The Administration's Cybersecurity Accomplishments* (Washington DC: The White House Blog, May 12, 2010).

[36] U.S. Director of National Intelligence Dennis C. Blair, *Annual Threat Assessment of the Intelligence Community for the House Permanent Select Committee on Intelligence* (Washington, DC: Director of National Intelligence, February 25, 2009).

[37] U.S. Director of National Intelligence James R. Clapper, *Worldwide Threat Assessment of the Intelligence Community for the House Permanent Select Committee on Intelligence* (Washington, DC: Director of National Intelligence, February 10, 2011).

[38] *Cybersecurity, Innovation, and the Internet Economy*, (Washington DC: Department of Commerce Internet Policy Task Force, June 2011).

[39] U.S. Deputy Secretary of Defense William F. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no.5 (September/October 2010): 100.

[40] National Security Council, *Cybersecurity Progress after President Obama's Address* (Washington, DC: The White House, July 14, 2010).

[41] *McAfee Threats Report: Second Quarter 2011* (Santa Clara CA: McAfee, 2011), 8.

[42] U.S. Secretary of Defense Robert M. Gates, *Submitted Statement to Senate Armed Services Committee* (Washington, DC: U.S. Senate, January 27, 2009), 8.

[43] U.S. Secretary of Defense Robert M. Gates, *Quadrennial Defense Review Report* (Washington, DC: Department of Defense, February 1, 2010): 2, 37-39.

[44] Kenneth Geers, *Cyberspace and the Changing Nature of Warfare,* Report IST-076/RSY-017 (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2008).

[45] Rex B. Hughes, "NATO and Cyber Defence: Mission Accomplished?" *Atlantisch Perspectief* 1 no. 4.

[46] Cooperative Cyber Defence Centre of Excellence, *Mission and Vision* (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence). http://transnet.act.nato.int/WISE/TNCC/CentresofE/CCD (accessed March 30, 2009).

[47] "Marching off to Cyber War," *The Economist* (print edition), December 4, 2008.

[48] Lynn, 97.

[49] Bradley Axmith, "American Drones Compromised by Virus," *Digital Journal*, October 9, 2011. http://www.digitaljournal.com/article/312544 (accessed on October 25, 2011).

[50] "Flying Operations of Remotely Piloted Aircraft Unaffected by Malware," Public Affairs Release Number 021011 (Peterson Air Force Base CO: Air Force Space Command, October 12, 2011).

[51] U.S. Secretary of Defense Robert M. Gates, "Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations," memorandum for Secretaries of the Military Departments, Washington, DC, June 23, 2009.

[52] *U.S. Cyber Command Fact Sheet* (Fort Meade MD: U.S. Cyber Command Public Affairs, October, 2011) http://www.stratcom.mil/factsheets/Cyber_Command (accessed on October 25, 2011).

[53] "DOD Announces First Strategy for Operating in Cyberspace," DoD News Release No. 608-11, (Washington DC: DoD, July 14, 2011).

[54] *Department of Defense Strategy for Operating in Cyberspace* (Washington DC: DoD, July 14, 2011).

[55] "Defending the Networks: The NATO Policy on Cyber Defence" (Brussels, Belgium: NATO Public Diplomacy Division, June 2011).

[56] "Hearing to Consider the Nomination of Hon. Leon E. Panetta to be Secretary of Defense," (Washington DC: U.S. Senate, Committee on Armed Services, June 9, 2011), 25.

[57] DoD defines cyberspace operations as "The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in and through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid." This also includes combatant commander consideration to use cyberspace operations as a means to achieve strategic or tactical objectives with effects in any domain. See: Vice Chairman of the Joint Chiefs of Staff General James E. Cartwright, "Definition of Cyberspace Operations," action memorandum for Deputy Secretary of Defense, Washington DC, September 29, 2008 (endorsed as approved on October 15, 2008).

[58] *Joint Operating Environment (JOE)* (Suffolk VA: U.S. Joint Forces Command), 3, 44. *Capstone Concept for Joint Operations (CCJO), Version 3.0* (Washington, DC: Department of Defense, January 15, 2009), 26, 31. Note that Figure 1 consists of summarized excerpts from the *JOE* and *CCJO.*

[59] James B. Michel et al., "Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System," *Proceedings of Twenty-seventh Annual International Software and Applications Conference* (Dallas, TX: Institute of Electrical and Electronics Engineers, November, 2003).

[60] See *Cyberspace Operations Concept Capability Plan 2016-2028*, TRADOC Pamphlet 525-7-8 (Fort Monroe, VA: U.S. Army Training and Doctrine Command, February 22, 2010) and *Cyberspace Operations*, Air Force Doctrine Document 3-12 (Maxwell AFB, AL: LeMay Center, July 15, 2010).

[61] Major General Rhett Hernandez (USA), *Statement of Incoming Commanding General, U.S. Army Forces Cyber Command Before the House Committee on Armed Services* (Washington DC, U.S. Congress, September 23, 2010).

[62] A.T. Mahan, *The Influence of Sea Power Upon History 1660-1783* (Mineola, NY: Dover, 1987 reprint), p 30: "The geographical position of a county may not only favor the concentration of its forces, but give the further strategic advantage of a central position and a good base for hostile operations against its probable enemies." Also see p.31-32.

[63] Martin Dodge and Rob Kitchin, *Atlas of Cyberspace* (Harlow, UK: Pearson Education Limited, 2001). Also, see K. Claffy et al., *Internet Mapping: from Art to Science* (San Diego, CA: Cooperative Association for Internet Data Analysis). *Joint Operating Environment (JOE),* 27. China's energy security is dependent on freedom of navigation through the Straits of Malacca, through which travels 80% of their oil imports.

[64] Major General Richard E. Webber (USAF), *Presentation to the House Armed Services Committee Subcommittee on Terrorism and Unconventional Threats* (Washington DC, U.S. Congress, September 23, 2010).

[65] *Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action* (Washington, DC: DHS, March 23, 2011).

[66] *Active Engagement, Modern Defence: Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation*, Adopted by Heads of State and Government in Lisbon (Lisbon, Portugal: NATO, November 19, 2010).

[67] Lynn, 99. See also *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: The National Academies Press, 2010).

[68] *International Strategy for Cyberspace,* 14.

[69] *The Comprehensive National Cybersecurity Initiative (CNCI)*, 3,4 and Lynn, 105.

II. STRATEGIES, GUIDANCE & DOCTRINE

This section includes:

- **National Strategy and Guidance**
- **Department of Defense Strategy and Guidance**
- **Joint Doctrine**
- **Service Doctrine**

This Page Intentionally Blank

National Strategy and Guidance

This section includes the:

- **U.S. International Strategy for Cyberspace**
- **National Framework for Strategic Communication**

This Page Intentionally Blank

U.S. International Strategy for Cyberspace

The White House Cybersecurity Coordinator released the International Strategy for Cyberspace, along with this factsheet, on 16 May 2011. The full strategy can be found at: http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf

INTERNATIONAL STRATEGY FOR CYBERSPACE
Prosperity, Security, and Openness in a Networked World

The U.S. International Strategy for Cyberspace outlines our vision for the future of cyberspace, and sets an agenda for partnering with other nations and peoples to realize it.

We live in a rare historical moment with an opportunity to build on cyberspace's successes and help secure its future—for the United States, and the global community.

Digital infrastructure is increasingly the backbone of prosperous economies, vigorous research communities, strong militaries, transparent governments, and free societies. The reach of networked technology is pervasive and global. To realize fully the benefits that networked technology promises the world, these systems must function reliably and securely. Assuring the free flow of information, the security and privacy of data, and the integrity of the interconnected networks themselves are all essential to American and global economic prosperity, security, and the promotion of universal rights.

Strategic Approach

The United States' approach to international cyberspace issues is founded on the belief that networked technologies hold immense potential for our Nation, and for the world. The United States will pursue an international cyberspace policy that stokes the innovation that drives our economy and improves lives here and abroad.

Our strategic approach builds on successes, recognizes the challenges to our national and economic security, and is always grounded by our unshakable commitments to fundamental freedoms of expression and association, privacy, and the free flow of information.

The Future We Seek

The cyberspace environment that we seek rewards innovation and empowers entrepreneurs; it connects individuals and strengthens communities; it builds better governments and expands accountability; it safeguards fundamental freedoms and enhances personal privacy; it builds understanding, clarifies norms of behavior, and enhances national and international security. This cyberspace is defined by four key characteristics:

- **Open** to innovation
- **Interoperable** the world over
- **Secure** enough to earn people's trust
- **Reliable** enough to support their work

To realize this vision, we will build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law. These norms include:

- Upholding Fundamental Freedoms
- Respect for Property
- Valuing Privacy
- Protection from Crime
- Right of Self-Defense
- Global Interoperability
- Network Stability
- Reliable Access
- Multi-stakeholder Governance
- Cybersecurity Due Diligence

To realize this future, the United States will combine diplomacy, defense, and development to enhance prosperity, security, and openness so all can benefit from networked technology.

Diplomacy: Strengthening Partnerships

The United States will work to create incentives for, and build consensus around, an international environment in which states – recognizing the intrinsic value of an open, interoperable, secure, and reliable cyberspace – work together and act as responsible stakeholders. Through our international relationships and affiliations, we will seek to ensure that as many stakeholders as possible are included in this vision of cyberspace precisely because of its economic, social, political, and security benefits.

Distributed systems require unified action because no single institution, document, arrangement, or instrument could suffice in addressing the needs of our networked world. From end-users, private- sector hardware and software vendors, and Internet service providers, to regional, multilateral, and multi-stakeholder organizations – all are important in helping cyberspace meet its full potential.

Defense: Dissuading and Deterring

The United States will, along with other nations, encourage responsible behavior and oppose those who would seek to disrupt networks and systems, thereby dissuading and deterring malicious actors, while reserving the right to defend these vital national assets as necessary and appropriate. The United States will continue to strengthen our network defenses and our ability to withstand and recover from disruptions and other attacks. For those more sophisticated attacks that do create damage, we will act on well-developed response plans to isolate and mitigate disruption to our machines, limiting effects on our networks, and potential cascade effects beyond them.

When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. We reserve the right to use all necessary means – diplomatic, informational, military, and economic – as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible.

Development: Building Prosperity and Security

We believe the benefits of a connected world are universal. The virtues of an open, interoperable, secure, and reliable cyberspace should be more available than they are today, and as the world's leading information economy, the United States is committed to ensuring others benefit from our technical resources and expertise.

Our Nation can and will play an active role in providing the knowledge and capacity to build and secure new and existing digital systems. The United States' capacity-building assistance is envisioned as an investment, a commitment, and an important opportunity for dialogue and partnership. As countries develop a stake in cyberspace issues, we intend our dialogues to mature from capacity- building to active economic, technical, law enforcement, defense and diplomatic collaboration on issues of mutual concern.

Policy Priorities

This strategy is an invitation to other states and peoples to join us in realizing this vision of prosperity, security, and openness in our networked world. It is a call to the private sector, civil society, and end- users to reinforce these efforts through partnership, awareness, and action. It is also a roadmap allowing the United States Government's departments and agencies to better define and coordinate their role in our international cyberspace policy, to execute a specific way forward, and to plan for future implementation.

The United States Government organizes its activities across seven interdependent areas of activity, each demanding collaboration within our government, with international partners, and with the private sector. Taken as a whole, they form the action lines of our strategic framework.

Economy: Promoting International Standards and Innovative, Open Markets
To ensure that cyberspace continues to serve the needs of our economies and innovators, we will:

- Sustain a free-trade environment that encourages technological innovation on accessible, globally linked networks.
- Protect intellectual property, including commercial trade secrets, from theft.
- Ensure the primacy of interoperable and secure technical standards, determined by technical experts.
- Protecting Our Networks: Enhancing Security, Reliability, and Resiliency
- Because strong cybersecurity is critical to national and economic security in the broadest sense, we will:
- Promote cyberspace cooperation, particularly on norms of behavior for states and cybersecurity, bilaterally and in a range of multilateral organizations and multinational partnerships.
- Reduce intrusions into and disruptions of U.S. networks.
- Ensure robust incident management, resiliency, and recovery capabilities for information infrastructure.
- Improve the security of the high-tech supply chain, in consultation with industry.

Law Enforcement: Extending Collaboration and the Rule of Law
To enhance confidence in cyberspace and pursue those who would exploit online systems, we will:

- Participate fully in international cybercrime policy development.
- Harmonize cybercrime laws internationally by expanding accession to the Budapest
- Convention.
- Focus cybercrime laws on combating illegal activities, not restricting access to the Internet.
- Deny terrorists and other criminals the ability to exploit the Internet for operational planning, financing, or attacks.
- Military: Preparing for 21st Century Security Challenges
- Since our commitment to defend our citizens, allies, and interests extends to wherever they might be threatened, we will:
- Recognize and adapt to the military's increasing need for reliable and secure networks.
- Build and enhance existing military alliances to confront potential threats in cyberspace.
- Expand cyberspace cooperation with allies and partners to increase collective security.

Internet Governance: Promoting Effective and Inclusive Structures
To promote Internet governance structures that effectively serve the needs of all Internet users, we will:

- Prioritize openness and innovation on the Internet.
- Preserve global network security and stability, including the domain name system (DNS).
- Promote and enhance multi-stakeholder venues for the discussion of Internet Governance issues.
- International Development: Building Capacity, Security, and Prosperity
- To promote the benefits of networked technology globally, enhance the reliability of our shared networks, and build the community of responsible stakeholders in cyberspace, we will:
- Provide the necessary knowledge, training, and other resources to countries seeking to build technical and cybersecurity capacity.
- Continually develop and regularly share international cybersecurity best practices.
- Enhance states' ability to fight cybercrime – including training for law enforcement, forensic specialists, jurists, and legislators.
- Develop relationships with policymakers to enhance technical capacity building, providing regular and ongoing contact with experts and their United States Government counterparts.

Internet Freedom: Supporting Fundamental Freedoms and Privacy
To help secure fundamental freedoms as well as privacy in cyberspace, we will:

- Support civil society actors in achieving reliable, secure, and safe platforms for freedoms of expression and association.
- Collaborate with civil society and nongovernment organizations to establish safeguards protecting their Internet activity from unlawful digital intrusions.
- Encourage international cooperation for effective commercial data privacy protections.
- Ensure the end-to-end interoperability of an Internet accessible to all.

These ideals are central to preserving the cyberspace we know, and to creating, together, the future we seek.

Updated: November 2011

National Framework for Strategic Communication

The National Framework for Strategic Communication was published in March 2010 pursuant to a requirement by Congress to provide a "comprehensive interagency strategy." It is clear, however, that this document is appropriately named. That is, it is a framework that outlines what strategic communication means to the Obama administration and how the executive branch of government organizes for and conducts the process that is strategic communication. The executive summary of the framework is presented below. The entire report can be found at: http://www.carlisle.army.mil/dime/documents/National%20Strategy%20for%20Strategic%20Communication.pdf

Purpose of Report
The Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 requires the President to submit to the appropriate committees of Congress a report on a comprehensive interagency strategy for public diplomacy and strategic communication.

Executive Summary
Across all of our efforts, effective strategic communications are essential to sustaining global legitimacy and supporting our policy aims. Aligning our actions with our words is a shared responsibility that must be fostered by a culture of communication throughout the government. We must also be more effective in our deliberate communication and engagement and do a better job understanding the attitudes, opinions, grievances, and concerns of peoples – not just elites – around the world.

Doing so is critical to allow us to convey credible, consistent messages, develop effective plans and to better understand how our actions will be perceived. Our study has revealed the need to clarify what strategic communication means and how we guide and coordinate our communications efforts. In this report, we describe "strategic communication" as the synchronization of our words and deeds as well as deliberate efforts to communicate and engage with intended audiences. We also explain the positions, processes, and interagency working groups we have created to improve our ability to better synchronize words and deeds and better coordinate communications and engagement programs and activities. These changes are already producing visible results; however, we still have much ground to cover.

We recognize the need to ensure an appropriate balance between civilian and military efforts. As a result, a process has been initiated to review existing programs and resources to identify current military programs that might be better executed by other Departments and Agencies. This process includes an interagency working group tasked to develop short-, medium-, and long-term options for addressing issues pertaining to budgets, personnel, and future programs and activities."

Updated: October 2011

This Page Intentionally Blank

Department of Defense Strategy and Guidance

This section includes the:

- **DoD Strategy for Operating in Cyberspace**
- **DoD Report on Strategic Communication**
- **DoD Principles of Strategic Communication**
- **DoD Directive (DoDD) 3600.01, Information Operations**

This Page Intentionally Blank

DoD Strategy for Operating in Cyberspace

The following is an excerpt from the DoD Strategy for Operating in Cyberspace (July 2011). The full strategy can be found at:
http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf

DoD's Strengths and Opportunities in Cyberspace

As does the nation as a whole, DoD relies on a secure and reliable cyberspace that protects fundamental freedoms, privacy, and the free flow of information. In support of both U.S. core commitments and national security, DoD has significant strengths and opportunities in cyberspace. The U.S. military's ability to use cyberspace for rapid communication and information sharing in support of operations is a critical enabler of DoD missions. More broadly, DoD's depth of knowledge in the global information and communications technology sector, including its cybersecurity expertise, provides the Department with strategic advantages in cyberspace.

Cyber Threats

The global scope of DoD networks and systems presents adversaries with broad opportunities for exploitation and attack. DoD must address vulnerabilities and the concerted efforts of both state and non-state actors to gain unauthorized access to its networks and systems. In developing its strategy for operating in cyberspace, DoD is focused on a number of central aspects of the cyber threat; these include:

- external threat actors,
- insider threats,
- supply chain vulnerabilities,
- and threats to DoD's operational ability.

Potential U.S. adversaries may seek to exploit, disrupt, deny, and degrade the networks and systems that DoD depends on for its operations. DoD is particularly concerned with three areas of potential adversarial activity:

- theft or exploitation of data;
- disruption or denial of access or service that affects the availability of networks, information, or network-enabled resources;
- and destructive action including corruption, manipulation, or direct activity that threatens to destroy or degrade networks or connected systems.

Strategic Initiative 1: DoD will treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential.

Though the networks and systems that make up cyberspace are man-made, often privately owned, and primarily civilian in use, treating cyberspace as a domain is a critical organizing concept for DoD's national security missions. This allows DoD to organize, train, and equip for cyberspace as we do in air, land, maritime, and space to support national security interests. Furthermore, these efforts must include the performance of essential missions in a degraded cyber environment.

As directed by the *National Security Strategy*, DoD must ensure that it has the necessary capabilities to operate effectively in all domains- air, land, maritime, space, and cyberspace. At all levels, DoD will organize, train, and equip for the complex challenges and vast opportunities of cyberspace. To this end, the Secretary of Defense has assigned cyberspace mission

responsibilities to United States Strategic Command (USSTRATCOM), the other Combatant Commands, and the Military Departments. Given its need to ensure the ability to operate effectively in cyberspace and efficiently organize its resources, DoD established U.S. Cyber Command (USCYBERCOM) as a sub-unified command of USSTRATCOM. The establishment of USCYBERCOM reflects DoD's need to:

- Manage cyberspace risk through efforts such as increased training, information assurance, greater situational awareness, and creating secure and resilient network environments;
- Assure integrity and availability by engaging in smart partnerships, building collective self defenses, and maintaining a common operating picture; and
- Ensure the development of integrated capabilities by working closely with Combatant Commands, Services, Agencies, and the acquisition community to rapidly deliver and deploy innovative capabilities where they are needed the most.

Strategic Initiative 2: DoD will employ new defense operating concepts to protect DoD networks and systems.

The implementation of constantly evolving defense operating concepts is required to achieve DoD's cyberspace mission today and in the future. As such, DoD has established a 5-step plan to form an adaptive and dynamic defense of DoD networks and systems:

- DoD is enhancing its cyber hygiene best practices to improve its cybersecurity.
- To deter and mitigate insider threats, DoD will strengthen its workforce communications, workforce accountability, internal monitoring, and information management capabilities.
- DoD will employ an active cyber defense capability to prevent intrusions onto DoD networks and systems.
- DoD is developing new defense operating concepts and computing architectures.

Strategic Initiative 3: DoD will partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy.

The challenges of cyberspace cross sectors, industries, and U.S. government departments and agencies; they extend across national boundaries and through multiple components of the global economy. Many of DoD's critical functions and operations rely on commercial assets, including Internet Service Providers (ISPs) and global supply chains, over which DoD has no direct authority to mitigate risk effectively. Therefore, DoD will work with the Department of Homeland Security (DHS), other interagency partners, and the private sector to share ideas, develop new capabilities, and support collective efforts to meet the crosscutting challenges of cyberspace.

DoD will continue to support the development of whole-of-government approaches for managing risks associated with the globalization of the information and communications technology sector. Many U.S. technology firms outsource software and hardware factors of production, and in some cases their knowledge base, to firms overseas. Additionally, increases in the number of counterfeit products and components demand procedures to both reduce risk and increase quality. Dependence on technology from untrusted sources diminishes the predictability and assurance that DoD requires, and DoD will work with DHS and its interagency partners to better identify and address these risks. The global technology supply chain affects mission critical aspects of the DoD enterprise, along with core U.S. government and private sector functions, and its risks must be mitigated through strategic public-private sector cooperation.

Strategic Initiative 4: DoD will build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity.

In support of the U.S. *International Strategy for Cyberspace* and in collaboration with its interagency partners, DoD will seek increasingly robust international relationships to reflect our core commitments and common interests in cyberspace. The development of international shared situational awareness and warning capabilities will enable collective self-defense and collective deterrence. By sharing timely indicators about cyber events, threat signatures of malicious code, and information about emerging actors and threats, allies and international partners can increase collective cyber defense. Cyberspace is a network of networks that includes thousands of ISPs across the globe; no single state or organization can maintain effective cyber defenses on its own.

Strategic Initiative 5: DoD will leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

The defense of U.S. national security interests in cyberspace depends on the talent and ingenuity of the American people. DoD will catalyze U.S. scientific, academic, and economic resources to build a pool of talented civilian and military personnel to operate in cyberspace and achieve DoD objectives. Technological innovation is at the forefront of national security, and DoD will foster rapid innovation and enhance its acquisition processes to ensure effective cyberspace operations. DoD will invest in its people, technology, and research and development to create and sustain the cyberspace capabilities that are vital to national security.

Conclusion

National security is being redefined by cyberspace. In addition to opportunities, DoD faces significant cyberspace challenges. The Department's military, intelligence, and business operations all depend upon cyberspace for mission success. The *Department of Defense Strategy for Operating in Cyberspace* assesses these challenges and opportunities and sets a strategic approach for DoD's cyber mission.

The Department's five strategic initiatives offer a roadmap for DoD to operate effectively in cyberspace, defend national interests, and achieve national security objectives. Each initiative is distinct, yet necessarily connected with the other four. Across the strategy, activities undertaken in one initiative will contribute to DoD's strategic thinking and lead to new approaches in the others.

By pursuing the activities in this strategy, DoD will capitalize on the opportunities afforded to the Department by cyberspace; defend DoD networks and systems against intrusions and malicious activity; support efforts to strengthen cybersecurity for interagency, international, and critical industry partners; and develop robust cyberspace capabilities and partnerships. This strategy will guide the Department's defense of U.S. interests in cyberspace so that the United States and its allies and partners may continue to benefit from the innovations of the information age.

Updated: October 2011

This Page Intentionally Blank

DoD Report on Strategic Communication

The Department of Defense Report on Strategic Communication was published in December 2009 pursuant to a requirement by Congress. Congress directed that the Secretary of Defense would report to the congressional defense committees on "the organizational structure within the Department of Defense for advising the Secretary on the direction and priorities for strategic communication activities, including an assessment of the option of establishing a board, composed of representatives from among the organizations within the Department responsible for strategic communications, public diplomacy, and public affairs, and including advisory members from the broader interagency community as appropriate, for purposes of (1) providing strategic direction for Department of Defense efforts related to strategic communications and public diplomacy; and (2) setting priorities for the Department of Defense in the areas of strategic communications and public diplomacy." The entire report can be found at: http://www.carlisle.army.mil/dime/documents/DoD%20report%20on%20Strategic%20Communication%20Dec%2009.pdf

Extract from the report

This report describes how DoD understands strategic communication, offers DoD views on the appropriate DoD role in strategic communication and public diplomacy, explains existing DoD processes and organizations that support effective strategic communication, and describes some potential future avenues for improvement and change (including an assessment of the option of establishing a strategic communication board within DoD).

Defining Strategic Communication for DoD

The *DoD Dictionary of Military and Associated Terms* (Joint Publication 1-02) defines the phrase "strategic communication" for the Department as "Focused United States Government efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of United States Government interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power." However, this recitation of a dictionary definition does not explain how this term is interpreted and implemented.

Emergent thinking is coalescing around the notion that strategic communication should be viewed as a process, rather than as a set of capabilities, organizations, or discrete activities. In its broadest sense, "strategic communication" is the process of integrating issues of audience and stakeholder perception into policy-making, planning, and operations at every level.

Other sections address DoD's role in strategic communication, the DoD strategic communication process, and key players and organizations involved in DoD strategic communication specifically at the national strategic level.

Updated: October 2011

This Page Intentionally Blank

DoD Principles of Strategic Communication

The following is an excerpt from a 15 August 2008 memo, which introduced the DoD Principles of Strategic Communication (signed by Robert T. Hastings, Principle Deputy Assistant Secretary of Defense for Public Affairs):

"Strategic Communication has been viewed as an emerging and extremely pertinent joint concept in recent years. Several important review panels have addressed Strategic Communication (SC) and the Chairman of the Joint Chiefs of Staff has designated Strategic Communication as one of the *CICS* Special Areas of Emphasis for joint education in 2007 and 2008.

Despite the interest and attention, Strategic Communication is still a developing concept. Contributing to the challenge is the lack of approved policy and doctrine.

As part of a larger DoD Strategic Communication education initiative, the Department held the first Strategic Communication Education Summit in March 2008, at the Joint Forces Staff College in Norfolk, Va. One of the most significant outcomes was the development of "Principles of Strategic Communication" to help standardize Strategic Communication education until policy and doctrine are published.

Through the collaborative efforts of DoD, State Department, and civilian educators and practitioners, the Principles initially developed in the Strategic Communication Education Summit have been refined into this guide. The purpose of this publication is to provide a tool to assist dialogue and instruction promoting understanding Strategic Communication.

As the Strategic Communication concept continues to mature, these Principles will be reviewed every two years until they are incorporated into *formal* doctrine. Comments are welcome and should be addressed to the Office of the Deputy Assistant Secretary of Defense for Joint Communication."

Principles of Strategic Communication

Definition of a principle: A fundamental tenet; a determining characteristic; an essential quality; an enduring attribute.

Strategic Communication (SC) has been described as the orchestration and/or synchronization of actions, images, and words to achieve a desired effect, yet there is more to understanding the concept.

As the joint force and agencies of the U.S. Government have begun executing Strategic Communication processes, common fundamentals have emerged. Through the collaborative efforts of DoD, State Department, civilian educators, and Strategic Communication practitioners, those common fundamentals have been consolidated and refined into nine principles of SC, described below. These principles are provided to assist dialogue and instruction promoting understanding of Strategic Communication.

Figure I below lists the nine principles of SC, with a short description of each. A more detailed explanation of each principle follows. The principles are not listed in any order of precedence.

Figure 1. Principles of Strategic Communication

Leadership-Driven. Leaders must decisively engage and drive the Strategic Communication process.
To ensure integration of communication efforts, leaders should place communication at the core of everything they do. Successful Strategic Communication - integrating actions, words, and images - begins with clear leadership intent and guidance. Desired objectives and outcomes are then closely tied to major lines of operation outlined in the organization, command or joint campaign plan. The results are actions and words linked to the plan. Leaders also need to properly resource strategic communication at a priority comparable to other important areas such as logistics and intelligence.

Credible. Perception of truthfulness and respect between all parties.
Credibility and consistency are the foundation of effective communication; they build and rely on perceptions of accuracy, truthfulness, and respect. Actions, images, and words must be integrated and coordinated internally and externally with no perceived inconsistencies between words and deeds or between policy and deeds. Strategic Communication also requires a professional force of properly trained, educated, and attentive communicators. Credibility also often entails communicating through others who may be viewed as more credible.

Understanding. Deep comprehension of attitudes, cultures, identities, behavior, history, perspectives and social systems. What we say, do, or show, may not be what others hear or see.

An individual's experience, culture, and knowledge provide the context shaping their perceptions and therefore their judgment of actions. We must understand that concepts of moral values are not absolute, but are relative to the individual's societal and cultural narrative. Audiences determine meaning by interpretation of our communication with them; thus what we say, do, or show, may not be what they hear or see. Acting without understanding our audiences can lead to critical misunderstandings with serious consequences.

Understanding subjective impacts of culture, language, history, religion, environment, and other factors is critical when crafting communication strategy for a relevant population. Building relationships and collaboration with the interagency, coalition, host nation, academic, non-profit, and business communities can facilitate better understanding of audiences.

Dialogue. Multi-faceted exchange of ideas to promote understanding and build relationships.

Effective communication requires a multi-faceted dialogue among parties. It involves active listening, engagement, and the pursuit of mutual understanding, which leads to trust. Success depends upon building and leveraging relationships. Leaders should take advantage of these relationships to place U.S. policies and actions in context prior to operations or events. Successful development and implementation of communication strategy will seldom happen overnight; relationships take time to develop and require listening, respect for culture, and trust-building.

Pervasive. Every action, image, and word sends a message.

Communication no longer has boundaries, in time or space. All players are communicators, wittingly or not. Everything the 10int Force says, does, or fails to do and say, has intended and unintended consequences. Every action, word, and image sends a message, and every team member is a messenger, from the 18-year-old rifleman to the commander. All communication can have strategic impact, and unintended audiences are unavoidable in the global information environment; therefore, leaders must think about possible "Nth" order communication results of their actions.

Unity of Effort. Integrated and coordinated, vertically and horizontally.

Strategic Communication is a consistent, collaborative process that must be integrated vertically from strategic through tactical levels, and horizontally across stakeholders. Leaders coordinate and synchronize capabilities and instruments of power within their area of responsibility, areas of influence, and areas of interest to achieve desired outcomes. Recognizing that your agency/organization will not act alone, ideally, all those who may have an impact should be part of communication integration.

Results-Based. Actions to achieve specific outcomes in pursuit of a well-articulated endstate.

Strategic communication should be focused on achieving specific desired results in pursuit of a clearly defined endstate. Communication processes, themes, targets and engagement modes are derived from policy, strategic vision, campaign planning and operational design. Strategic communication is not simply "another tool in the leader's toolbox," but must guide all an organization does and says; encompassing and harmonized with other functions for desired results.

Responsive. Right audience, right message, right time, and right place.
Strategic Communication should focus on long-term end states or desired outcomes. Rapid and timely response to evolving conditions and crises is important as these may have strategic effects. Communication strategy must reach intended audiences through a customized message that is relevant to those audiences. Strategic Communication involves the broader discussion of aligning actions, images, and words to support policy, overarching strategic objectives and the longer term big picture. Acting within adversaries' decision cycles is also key because tempo and adaptability count. Frequently there will be a limited window of opportunity for specific messages to achieve a desired result.

An organization must remain flexible enough to address specific issues with specific audiences, often at specific moments in time, by communicating to achieve the greatest effect. All communication carries inherent risk and requires a level of risk acceptance within the organization. Leaders must develop and instill a culture that rewards initiative while not overreacting to setbacks and miscues. While risk must be addressed in the form of assumptions in planning, it should not restrain leaders' freedom of action providing it has been taken into consideration appropriately.

Continuous. Diligent ongoing research, analysis, planning, execution, and assessment that feeds planning and action.
Strategic Communication is a continuous process of research and analysis, planning, execution, and assessment. Success in this process requires diligent and continual analysis and assessment feeding back into planning and action. Strategic Communication supports the organization's objectives by adapting as needed and as plans change. The SC process should ideally operate at a faster tempo or rhythm than our adversaries.

Updated: October 2011

Department of Defense Directive (DoDD) 3600.01 Information Operations

The following is an excerpt from Department of Defense Directive (DODD) 3600.01, "Information Operations" (14 August 2006, Change 1 incorporated 23 May 2011). The full directive can be found at: http://www.dtic.mil/whs/directives/corres/dir.html.

Purpose. DoDD 3600.1 is the *fundamental* document for both understanding and employing Information Operations (IO). As such it should be the starting point for all study of Information Operations as undertaken by U.S. practitioners. This directive establishes IO policy, definitions, and responsibilities in the Department of Defense (DOD) to support the objective of making IO a core military competency. It also directs the coordination and deconfliction of information gathering activities in support of IO and Human Intelligence (HUMINT) and other intelligence activities within the Combatant Commands.

Information Operations (IO) Definition. The definition included in this directive has been superseded by the SecDef Memo 12401-10 (25 January 2011). The following shows both the original and updated definitions (additions – underline and deletions – strike through). "The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation ~~of the core capabilities of Electronic Warfare (EW), Computer Network Operations (CNO), Military Information Support Operations (MISO), Military Deception (MILDEC), and Operations Security (OPSEC), in concert with specified supporting and related capabilities,~~ to influence, disrupt, corrupt, or usurp ~~adversarial human and automated~~ the decision making of adversaries and potential adversaries while protecting our own."

IO Policy. IO shall be employed to support full spectrum dominance by taking advantage of information technology, maintaining U.S. strategic dominance in network technologies, and capitalizing upon near real-time global dissemination of information, to affect adversary decision cycles with the goal of achieving information superiority for the United States.

Core IO Capabilities. IO employs five core capabilities to achieve desired Combatant Commander effects or prevent the enemy from achieving his desired effects: EW, CNO, MISO, MILDEC, and OPSEC. They are operational in a direct and immediate sense; they either achieve critical operational effects or prevent the adversary from doing so. They are interdependent and increasingly need to be integrated to achieve desired effects.

Supporting Capabilities (See Glossary for definitions):

- Counterintelligence (CI)
- Human Intelligence (HUMINT)
- Physical (kinetic) attack
- Physical Security
- Information Assurance (IA)
- Combat Camera

Related Capabilities (See Glossary for definitions):

- Public Affairs (PA)
- Civil-Military Operations (CMO)
- Defense Support to Public Diplomacy (DSPD)

Intelligence Support. Intelligence will be developed, consistent with the National Intelligence Priorities Framework, to provide data about adversary information systems or networks; produce political-military assessments; conduct human factors analysis; and provide indications and warning of adversary IO, including threat assessments.

Other Human-Derived Information Gathering Activities. Provide "atmospherics" in support of IO and include polling, surveys, opinion research, spot reports, and consolidation of other information relevant to prevailing moods, attitudes, and influences among a population. These activities for atmospherics in support of IO planning and execution shall be coordinated and deconflicted with the Intelligence Community (IC). All contracts to support human-derived information gathering activities shall have proper USG oversight and undergo a policy review.

Responsibilities. The following officials, commands, and agencies are tasked with the specific responsibilities indicated:

Under Secretary of Defense for Intelligence (USD(I)):

- Serve as the Principal Staff Assistant to the Secretary of Defense for IO.
- Develop and oversee DOD IO policy and integration activities.
- Assess performance/responsiveness of DOD and Military Intelligence activities to support IO.
- Serve as the DOD lead within the IC regarding IO issues, and provide guidance for the coordination and deconfliction of HUMINT and related intelligence activities and other human-derived information gathering activities.
- Coordinate, oversee, and assess the efforts of the DOD Components to plan, program, develop, and execute capabilities in support of IO requirements.
- Establish specific policies for the development and integration of CNO, MILDEC and OPSEC as core IO capabilities.

Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)):

- Establish specific policies for the development and integration of EW as a core IO capability.
- Develop and maintain a technology investment strategy for development, acquisition, and integration of EW capabilities.
- Invest in and develop the science and technologies needed to support IO capabilities.

The Under Secretary of Defense for Policy (USD(P)):

- Provide DOD oversight of IO planning, execution, and related policy guidance including the establishment of an OSD review process to assess IO plans and programs.
- Lead interagency coordination, exclusive of the IC, and international cooperation involving planning and employment of IO capabilities.
- Establish specific policy and oversight for development and integration of MISO as a core IO capability and DSPD as a related capability.

The Under Secretary of Defense for Personnel and Readiness (USD(P&R)):

- Develop policy and procedures on matters pertaining to the establishment and management of an IO career force in coordination with the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, the USD(P), the USD(I), and others, as appropriate.
- Provide training policy and oversight as it pertains to the integration of all IO capabilities into joint exercises and joint training regimes.

The Assistant Secretary of Defense for Networks and Information Integration/ DOD Chief Information Officer (ASD(NII)/DOD CIO) will:

- Establish specific policy for the development and integration of IA and Computer Network Defense (CND) as related to CNO as a core IO capability.
- Oversee and assess the efforts of the Heads of the DOD Components to plan, program, develop, and field IA and CND capabilities in support of CNO.

Assistant Secretary of Defense for Public Affairs will:

- Establish specific policy for the relationship of PA to IO.
- Oversee PA planning and coordination efforts as related to IO within DOD.
- Oversee the development and conduct of appropriate training and education that defines PA's relationship to IO for public affairs and visual information personnel at the Defense Information School.

Commander, U.S. Strategic Command (CDRUSSTRATCOM):

- Integrate and coordinate DOD IO core capabilities that cross geographic areas of responsibility or core IO areas.

Commander, U.S. Special Operations Command (CDRUSSOCOM):

- Integrate and coordinate DOD MISO capabilities to enhance interoperability and support USSTRATCOM's information operations responsibilities and other combatant commanders' MISO planning and execution.
- Support the other Combatant Commanders though joint employment of MISO and other special operations force IO capabilities.
- Employ other special operations force IO capabilities as directed.

The Secretaries of the Military Departments and CDRUSSOCOM:

- Develop IO doctrine and tactics, and organize, train, and equip for IO for their Title 10 (U.S. Code) and Major Force Program responsibilities.

The Chairman of the Joint Chiefs of Staff:

- Serve as the principal military advisor to the President of the United States, the National Security Council, and the Secretary of Defense on IO.
- Validate capability-based IO requirements through the Joint Requirements Oversight Council.
- Develop and maintain joint doctrine for core, supporting, and related IO capabilities in joint operations.
- Ensure all joint education, training, plans, and operations include, and are consistent with, IO policy, strategy, and doctrine.

Updated: October 2011

This Page Intentionally Blank

Joint Doctrine

Joint Information Operations Doctrine

Key doctrinal documents:

- Joint Pub 3-13, *Information Operations*, 13 February 2006
- Joint Pub 3-13.1, *Electronic Warfare*, 25 January 2007
- Joint Pub 3-13.2, Psychological Operations, 07 January 2010
- Joint Pub 3-13.3, *Operations Security*, 29 June 2006
- Joint Pub 3-13.4, *Military Deception*, 13 July 2006
- Joint Pub 3-57, *Civil-Military Operations*, 08 July 2008
- Joint Pub 3-61, *Public Affairs*, 25 August 2010

Joint Pubs available at: http://www.dtic.mil/doctrine/s_index.html
and at https://jdeis.js.mil/jdeis/index.jsp.

Joint Information Operations doctrine is set down in Joint Publication 3-13. This section extracts the publication's executive summary below:

EXECUTIVE SUMMARY, JOINT PUBLICATION 3-13

- **Discusses the Information Environment and Its Relationship to Military Operations**
- **Discusses the Information Operations (IO) Core Capabilities Necessary to Successfully Plan and Execute IO to include Supporting and Related Capabilities in a Joint/Multinational Environment**
- **Aligns Joint IO Doctrine with the Transformational Planning Guidance as Specified by the Department of Defense IO Roadmap for Achieving Information Superiority on the Battlefield**
- **Provides an Organizational Framework for Integrating, Deconflicting, and Synchronizing IO Planning and Execution Activities for Supporting and Supported Combatant Command Staffs, National Intelligence Agencies, and Other Federal Agencies as Applicable**
- **Outlines Planning Considerations for Developing an IO Career Force through Joint Education, Training, Exercises, and Experimentation**

NOTE: The definition included in this publication has been superseded by the SecDef Memo 12401-10 (25 January 2011). The term psychological operations (PSYOP) has been replaced by military information support operations (MISO). The following shows both the original and updated information (additions – underline and deletions – strike through).

Military Operations and the Information Environment

To succeed, it is necessary for US forces to gain and maintain information superiority.

Information is a strategic resource, vital to national security, and military operations depend on information and information systems for many simultaneous and integrated activities.

Information operations (IO) are described as the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation ~~of the core capabilities of Electronic Warfare (EW), Computer Network Operations (CNO), Military Information Support Operations (MISO), Military Deception (MILDEC), and Operations Security (OPSEC), in concert with specified supporting and related capabilities,~~ to influence, disrupt, corrupt, or usurp ~~adversarial human and automated~~ the decision making of adversaries and potential adversaries while protecting our own.

The purpose of this doctrine is to provide joint force commanders (JFCs) and their staffs guidance to help prepare, plan, execute, and assess IO in support of joint operations. The principal goal is to achieve and maintain information superiority for the US and its allies.

The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. The information environment is made up of three interrelated dimensions: physical, informational, and cognitive.

Core, Supporting, and Related Information Operations Capabilities

Core capabilities.

IO consists of five core capabilities which are: ~~PSYOP~~ MISO, MILDEC, OPSEC, EW, and CNO. Of the five, ~~PSYOP~~ MISO, OPSEC, and MILDEC have played a major part in military operations for many centuries. In this modern age, they have been joined first by EW and most recently by CNO. Together these five capabilities, used in conjunction with supporting and related capabilities, provide the JFC with the principal means of influencing an adversary and other target audiences (TAs) by enabling the joint forces freedom of operation in the information environment.

Supporting capabilities.

Capabilities supporting IO include information assurance (IA), physical security, physical attack, counterintelligence, and combat camera. These are either directly or indirectly involved in the information environment and contribute to effective IO. They should be integrated and coordinated with the core capabilities, but can also serve other wider purposes.

Related capabilities.

There are three military functions: public affairs (PA), civil military operations (CMO), and defense support to public diplomacy, specified as **related capabilities for IO**. These capabilities make significant contributions to IO and must always be coordinated and integrated with the core and supporting Information Operations capabilities. However, their primary purpose and rules under which they operate must not be compromised by IO. This requires additional care and consideration in the planning and conduct of IO. For this reason, the PA and CMO staffs particularly must work in

close coordination with the IO planning staff.

Intelligence and Communications System Support to Information Operations

Successful planning, preparation, execution, and assessment of information operations (IO) demand detailed and timely intelligence.

Before military activities in the information environment can be planned, the current "state" of the dynamic information environment must be collected, analyzed, and provided to commanders and their staffs. This requires intelligence on relevant portions of the physical, informational, and cognitive properties of the information environment, which necessitates collection and analysis of a wide variety of information and the production of a wide variety of intelligence products.

Nature of IO intelligence requirements.

In order to understand the adversary or other TA decision-making process and determine the appropriate capabilities necessary to achieve operational objectives, commanders and their staffs must have current data. This includes relevant physical, informational, and cognitive properties of the information environment as well as assessment of ongoing IO activities.

Intelligence considerations in planning IO.

Intelligence Resources are Limited. Commanders and their intelligence and operations directorates must work together to identify IO intelligence requirements and ensure that they are given high enough priority in the commander's requests to the intelligence community (IC).

Collection Activities are Legally Constrained. The IC must implement technical and procedural methods to ensure compliance with the law. Additionally, intelligence may be supplemented with information legally provided by law enforcement or other sources.

Intelligence Support to IO Often Requires Long Lead Times. The intelligence necessary to affect adversary or other TA decisions often requires that specific sources and methods be positioned and employed over time to collect the necessary information and conduct the required analyses.

Information Environment is Dynamic. Commanders and their staffs must understand both the timeliness of the intelligence they receive and the differing potentials for change in the dimensions of the information environment.

Properties of the Information Environment Affect Intelligence. Collection of physical and electronic information is objectively measurable by location and quantity. Commanders and their staffs must have an appreciation for the subjective nature of psychological profiles and human nature.

Joint Staff. **The Chairman's responsibilities for IO** are both general (such as those to establish doctrine, provide advice, and make recommendations) and specific (such as those assigned in DOD IO policy). The Operations Directorate of the Joint Staff (J-3) serves as the Chairman's focal point for IO and coordinates with the other organizations within the Joint Staff that have direct or supporting IO responsibilities. The IO divisions of the Joint Staff J-3 provide IO specific advice and advocate Joint Staff and combatant commands' IO interests and concerns within DOD and interact with other organizations and individuals on behalf of the Chairman.

Combatant commands. Commander, United States Strategic Command's (USSTRATCOM's) specific authority and responsibility to coordinate IO across area of responsibility (AOR) and functional boundaries does not diminish **the imperative for other combatant commanders to employ IO**. These efforts may be directed at achieving national or military objectives incorporated in theater security cooperation plans, shaping the operational environment for potential employment during periods of heightened tensions, or in support of specific military operations. It is entirely possible that in a given theater, the combatant commander will be supported for select IO while concurrently supporting USSTRATCOM IO activities across multiple theater boundaries.

Components. **Components** are normally responsible for detailed planning and execution of IO. IO planned and conducted by functional components must be conducted within the parameters established by the JFC. At the same time, component commanders and their subordinates must be provided sufficient flexibility and authority to respond to local variations in the information environment. Component commanders determine how their staffs are organized for IO, and normally designate personnel to liaise between the JFC's headquarters and component headquarter staffs.

Subordinate joint force commanders. Subordinate JFCs plan and execute IO as an integrated part of joint operations. Subordinate staffs normally share the same type of relationship with the parent joint force IO staff as the Service and functional components. **Subordinate JFC staffs may become involved in IO planning and execution to a significant degree**, to include making recommendations for employment of specific capabilities, particularly if most of the capability needed for a certain operation resides in that subordinate joint task force.

Organizing for joint IO. Combatant commanders normally **assign responsibility for Information Operations** to the **J-3**. When authorized, the director of the J-3 has primary staff responsibility for planning, coordinating, integrating, and assessing joint force IO. **The J-3 normally designates an Information Operations cell chief** to assist in executing joint IO responsibilities. The primary function of the IO cell chief is to ensure that IO are integrated and synchronized in all planning processes of the combatant command staff and that IO

aspects of such processes are coordinated with higher, adjacent, subordinate, and multinational staffs. To integrate and synchronize the core capabilities of IO with IO-supporting and related capabilities and appropriate staff functions, the IO cell chief normally leads an "IO cell" or similarly named group as an integrated part of the staff's operational planning group or equivalent. The organizational relationships between the joint IO cell and the organizations that support the IO cell are per JFC guidance.

Planning and Coordination

IO planning follows the same principles and processes established for joint operation planning.

The IO staff coordinates and synchronizes capabilities to accomplish JFC objectives. Uncoordinated IO can compromise, complicate, negate, or harm other JFC military operations, as well as other USG information activities. JFCs must ensure Information Operations planners are fully integrated into the planning and targeting process, assigning them to the joint targeting coordination board in order to ensure full integration with all other planning and execution efforts. Other USG and/or coalition/allied information activities, when uncoordinated, may complicate, defeat, or render DOD IO ineffective. Successful execution of an information strategy also requires early detailed JFC IO staff planning, coordination, and deconfliction with USG interagency efforts in the AOR to effectively synergize and integrate IO capabilities.

Planning considerations.

IO planning must begin at the **earliest stage** of a JFC's campaign or operations planning and must be an integral part of, not an addition to, the overall planning effort. IO are used in all phases of a campaign or operation. The use of IO during early phases can significantly influence the amount of effort required for the remaining phases.

The use of IO in peacetime to achieve JFC objectives and to preclude other conflicts, requires an ability to integrate Information Operations capabilities into a comprehensive and coherent strategy through the establishment of information objectives that in turn are integrated into and support the JFC's overall mission objectives. The combatant commander's theater security cooperation plan serves as an excellent platform to embed specific long-term information objectives.

IO planning requires early and detailed preparation. Many Information Operations capabilities require long lead-time intelligence preparation of the battlespace (IPB). IO support for IPB development differs from traditional requirements in that it may require greater lead time and may have expanded collection, production, and dissemination requirements. Consequently, combatant commanders must ensure that IO objectives are appropriately prioritized in their priority intelligence requirements (PIRs) and requests for information (RFIs).

As part of the planning process, designation of release and execution authority is required. Release authority provides the approval for IO employment and normally specifies the allocation of

specific offensive means and capabilities provided to the execution authority. Execution authority is described as the authority to employ IO capabilities at a designated time and/or place. Normally, the JFC is the one execution authority designated in the execute order for an operation.

IO may involve complex legal and policy issues requiring careful review and national-level coordination and approval.

Commander's intent and information operations.

The commander's vision of IO's role in an operation should begin before the specific planning is initiated. A commander that expects to rely on IO capabilities must ensure that IO related PIRs and RFIs are given high enough priority prior to a crisis, in order for the intelligence products to be ready in time to support operations. At a minimum, the commander's vision for IO should be included in the initial guidance. Ideally, commanders give guidance on Information Operations as part of their overall concept, but may elect to provide it separately.

Measures of performance and measures of effectiveness.

Measures of performance (MOPs) gauge accomplishment of Information Operations tasks and actions. **Measures of effectiveness (MOEs)** determine whether IO actions being executed are having the desired effect toward mission accomplishment: the attainment of end states and objectives. MOPs measure friendly IO effort and MOEs measure battlespace results. IO MOPs and MOEs are crafted and refined throughout the planning process.

Multinational Considerations in Information Operations

Every ally/coalition member can contribute to IO by providing regional expertise to assist in planning and conducting IO.

Allies and coalition partners recognize various IO concepts and some have thorough and sophisticated doctrine, procedures, and capabilities for planning and conducting IO. **The multinational force commander is responsible to resolve potential conflicts** between each nation's IO programs and the IO objectives and programs of the coalition. It is vital to integrate allies and coalition partners into IO planning as early as possible so that an integrated and achievable IO strategy can be developed early in the planning process.

Integration requirements include clarification of allied and coalition partner's IO objectives; understanding of other nations' information operations and how they intend to conduct IO; establishment of liaison/deconfliction procedures to ensure coherence; and early identification of multinational force vulnerabilities and possible countermeasures to adversary attempts to exploit them.

Information Operations in Joint Education, Training, Exercises, and Experiments

A solid foundation of education and training is essential to the development of IO core competencies.

The development of IO as a core military competency and critical component to joint operations requires specific expertise and capabilities at all levels of DOD. At the highest professional levels, senior leaders develop joint warfighting core competencies that are the capstone to American military power. The Services, United States Special Operations Command, and other agencies develop capabilities oriented on their core competencies embodied in law,

policy, and lessons learned. At each level of command, a solid foundation of education and training is essential to the development of a core competency. Professional education and training, in turn, are dependent on the accumulation, documentation, and validation of experience gained in operations, exercises, and experimentation.

IO education considerations.

The IO career force should consist of both capability specialists (EW, ~~*PSYOP*~~ *MISO*, CNO, MILDEC, and OPSEC) and IO planners. Both groups require an understanding of the information environment, the role of IO in military affairs, how IO differs from other information functions that contribute to information superiority, and specific knowledge of each of the core capabilities to ensure integration of IO into joint operations.

IO planners are required at both the component and the joint level.

Senior military and civilian DOD leaders require an executive level knowledge of the information environment and the role of IO in supporting DOD missions.

IO training considerations.

Joint military training is based on joint policies and doctrine to prepare joint forces and/or joint staffs to respond to strategic and operational requirements deemed necessary by combatant commanders to execute their assigned missions.

IO training must support the IO career force and be consistent with the joint assignment process. Joint IO training focuses on joint planning- specific skills, methodologies and tools, and assumes a solid foundation of Service-level IO training.

The Services determine applicable career training requirements for both their IO career personnel and general military populations, based on identified joint force mission requirements.

CONCLUSION

This document [JP 3-13] provides the doctrinal principles for DOD employment of IO. It has been designed to provide overarching guidance in the planning and execution of IO in today's joint/ multinational security environment. Its primary purpose is to ensure all of the capabilities comprising IO are effectively coordinated and integrated into our nation's warfighting capability against current and future threats.

Updated: October 2011

This Page Intentionally Blank

Service Doctrine

This section includes the:

- **Army Information Doctrine**
- **Marine Corps Information Doctrine**
- **Navy Information Doctrine**
- **Air Force Information Doctrine**

This Page Intentionally Blank

Army Information Doctrine

Key doctrinal documents: FM 6-0 *Mission Command* (June 2011), Army Doctrine Publication (ADP) and Army Doctrine Reference Publication (ADRP) 6-0, *Mission Command* (TBP) and FM 3-13, *Inform and Influence Activities* (TBP)

Army forces conduct unified land operations in populated areas that require them to contend with the attitudes and perceptions of many audiences within and beyond their area of operations. Field Manual 6-0, *Mission Command*, (June 2011) established the new Mission Command warfighting function (MC WfF) and launched the Army's evolution of information operations to Inform and Influence Activities (IIA). These activities support and enhance current joint information operations doctrine that, by definition, remains focused on adversaries and potential adversaries only. Inform and Influence Activities focus on all audiences within the information environment, which include domestic, foreign friendly and neutral, adversary and enemy. It is also in line with the new definition for IO and emerging joint doctrine as it also enables commanders with multiple information-related capabilities and allows them to evaluate and use available internal and request external resources to inform or influence selected populaces, actor or audiences as desired to support his or her mission objectives. They do this through *Inform and Influence Activities*—the integration of designated information-related capabilities in order to synchronize themes, messages and actions with operations to inform U.S. and global audiences; influence foreign audiences; and affect adversary and enemy decision making. (FM 6-0)

Two mission command warfighting function tasks replaced the Army's previous five information tasks: information engagement, command and control warfare, information protection, operations security, and military deception. The commander's task is to lead Inform and Influence Activities, which includes: collaborating with the staff, subordinate commanders and unified action partners; establishing themes and messages; and personally engaging key target audiences and individuals.

The staff task is to conduct Inform and Influence Activities. This single category activity is solely focused on integration both horizontally and vertically among the staff elements to assist the commander with developing and synchronizing themes and messages with actions to support operations. Ultimately, this supports the commander's efforts to shape the operational environment, as well as to avoid message contradiction or such perception, which could lead to information fratricide and thus undermine the operation. Commanders employ information-related capabilities within their areas of operation to inform audiences, build trust and confidence, promote support for Army operations, and ultimately persuade and influence perceptions and behavior.

Information-Related Capabilities are tools and techniques utilizing a dimension(s) within the Information Environment, which can be used to generate an end(s). End(s) is an outcome(s) that results because of the way capabilities are applied. (Joint Staff)

All assets and capabilities at a Commander's disposal have the capacity to inform and influence to varying degrees. Most are information-centric in mission and purpose and are designed, trained and resourced to inform, influence or both. Commanders and staffs, however, are not limited to these information-related capabilities when planning operations. Inform and influence activities recognize that success depends on effectively employing ALL assets in order to shape the information environment as depicted in the figure below, so that themes, messages and actions are synchronized with each other and with operations. In addition to the information-related capabilities the Commander can designate other capabilities not solely designed to inform or influence, such as maneuver forces, engineers, medical units and other assets to achieve mission objectives.

Information-Related Capabilities within Inform and Influence Activities include:

- Public Affairs
- Military Information Support Operations
- Soldier and Leader Engagement
- Combat Camera
- Military Deception
- Cyber Electromagnetic Activities (Electronic Warfare, Computer Network Operations, Network Operations, Information Security)
- Operations Security
- Civil Affairs Operations
- Special Technical Operations
- Commander designated enablers (other)

Integration of Information-Related Capabilities to affect the Information Environment

Inform and influence activities has two lines of effort, the inform line of effort and the influence line of effort. These two lines of effort enable commanders to achieve the mission command objectives and maintain statutory requirements. The inform line of effort provides accurate and factual information to domestic and foreign audiences. Maintaining transparency and credibility is critical within this line of effort. The inform line of effort includes public affairs (at home and abroad), military information support operations (abroad), and Soldier and leader engagement (at home and abroad).

The influence line of effort activities serve to effectively change attitudes, beliefs, and ultimately the behavior of foreign friendly, neutral, adversary and enemy populaces and target audiences to support operations. The goal is to guide others to make decisions or act in a way that supports the commanders' objectives. The influence line of effort integrates actions designed to extend influence among foreign partners and the local populace within the unit areas of operation. It includes military information support operations, Soldier and leader engagement, and military deception activities. Although each line of effort has a different task and purpose, multiple information-related capabilities could employ to support the same objectives in a reinforcing manner.

Public Affairs

Public Affairs fulfills the Army's obligation to keep the American people and the Army informed, and helps to establish the conditions that lead to confidence in America's Army and its readiness to conduct operations in peacetime, conflict and war. (FM 46-1)

Public Affairs communicate with internal and external Army publics about Army operations and responsibilities to enhance public understanding and garner U.S., as well as global support for the Army. It fulfills the legal mandate to inform the American people about the Army's mission and goals – to communicate to the public what the Army does.

Public Affairs synchronization with other information-related capabilities helps the commander shape the information environment and counter enemy propaganda and disinformation. It assists the commander in the development of themes and messages and collaborates with other information-related capabilities to protect operational security and avoid information fratricide.

Public Affairs participates in the information integration process within the Inform and Influence Activities Element in a number of ways:

- Assists the commander to develop themes and messages.
- Prepares and rehearses the commander and other leaders to conduct press conferences or interviews.
- Servers as the commander's spokesperson, when required.
- Conducts ongoing media assessments to determine the degree and nature of media coverage; takes steps to correct misinformation or propaganda.
- Conducts ongoing background research in order to provide accurate context and information.
- Ensures public affairs planning from the outset of operations.
- Seeks to leverage other information-related capabilities, such as combat camera or civil affairs, to provide greater accuracy and breadth of information.
- Cultivates relationships with the media and engages them candidly and consistently.
- Ensures coordination with other information-related capabilities to avoid information fratricide.

For additional guidance on Public Affairs, see FM 46-1 *Public Affairs Operations*.

Military Information Support Operations

Military Information Support Operations is the commander's primary dedicated capability to inform and influence foreign populations within the operational area. Military Information Support Operations is conducted to induce or reinforce specific attitudes and behaviors that are favorable to U.S. military objectives. When Military Information Support Operations is integrated properly across the range of military operations, the risk to U.S. forces is lessened and collateral damage and expenditures of assets are significantly reduced.

Military information support (MIS) forces are organized, trained and equipped to plan, resource, and conduct Military Information Support Operations. They support Soldier and leader engagement, as well as military deception, as required or tasked. They also advise commanders and their staffs on the cognitive and psychological effects of military operations, as well as unintended psychological impacts of actions, and recommend effective messages and actions for delivery to achieve the commander's intent through influence.

Military Information Support Operations participates in the information integration process within the Inform and Influence Activities Element in a number of ways:

- Advises the commander and Chief of Mission (COM) on the psychological effects of military actions and country team or host/partner nation (HN/PN) information programs in the operational areas and on targeting to maximize effects and minimize adverse impact and unintended consequences.
- Influences foreign populations through relevant and credible messages, activities, and actions targeting select individuals and populations to affect decision making and subsequent behavior changes in support of U.S. national and military objectives. This includes by use of Military Information Support Operations, Military deception, and Soldier/leader engagement.
- Delivers information to target audiences to inform, influence, and direct.
- Plans, coordinates, and employs Military Information Support Operations unilaterally and in conjunction with allies, coalition partners, host/partner nation (HN/PN), and friendly indigenous personnel.
- Trains, advises, and assists government organizations and security forces to establish host/partner nation (HN/PN) information capabilities, through unified action and security assistance measures, to facilitate interoperability and host/partner nation (HN/PN) self-sustainment.
- Disseminates public service information during civil support and humanitarian assistance operations to reestablish or reinforce legitimacy, ease suffering, and maintain or restore civil order.
- Assesses information delivered to gain and hold the initiative to support the narrative.
- Assesses adversary information, including information for effect (IFE), misinformation, disinformation and propaganda in conjunction with the G2 (S2), G7/Inform and Influence Activities Officer and Public Affairs Officer to determine the source, intent, intended target, and effects; analyze and assess the feasibility, necessity and best method(s) to counter the effects; and as required, develop and deliver timely counter-information to hold the initiative and convey friendly intent and actions.
- Collects relevant information to enhance the commander's understanding of the operational environment and to facilitate his decision-making in applying military actions through direct and indirect observations and insights into the attitudes, perceptions, and behaviors of target audiences.

For more information on Military Information Support Operations see FM 3-05.30 and FM 3-05.301.

Soldier and Leader Engagement
Soldier and leader engagement broadly describes interactions that take place among Soldiers, leaders and audiences or individuals within the area of operations. Soldier and leader engagements can occur as dynamic (impromptu or chance), face-to face encounters on the street, or as deliberate scheduled meetings. Such engagements can also employ other means, such as phone calls, video-teleconference or other media.

Soldier and leader engagement is a component of a larger engagement strategy that includes public affairs engagements, especially with the media; civil military operations or civil affairs engagements, such as medical civil action programs (MEDCAPs); and civil-military engagements, such as those in support of security force assistance efforts.

Given its importance to Inform and Influence Activities and current lack of doctrine regarding Soldier/leader engagement, a more comprehensive overview of this information-related capability is provided in FM 3-13, Chapter 5.

Combat Camera
Combat Camera provides commanders with a directed imagery capability in support of operational and planning requirements through the full range of military operations.

Combat Camera forces perform unique and highly specialized missions with Video Documentation capabilities supporting all phases of an operation or campaign. Combat Camera teams are trained and equipped to access events and areas unavailable to other VI personnel or media representatives. Combat Camera personnel maintain qualifications enabling them to operate with airborne forces, air crew, special operations forces (SOF), and military divers. Their capabilities range from aerial photography to underwater photography. Furthermore, Combat Camera teams have a technological capability for the timely transmission of images during fast-moving operations and support forward-operating maneuver elements.

Army COMCAM units are under the operational control of US Forces Command (FORSCOM) until they are deployed. Army capabilities include the following:

- Tactical Digital Media.
- Editing capabilities.
- Transmission for conventional non-conventional and airborne operations.
- High Definition Camera equipment.

Combat Camera participates in the information integration process within the Inform and Influence Activities Element in a number of ways:

- Provides real-time imagery to support the commander's messaging efforts.
- Accurately portrays U.S. forces in action in order to reinforce other inform capabilities.
- Documents operations and provides imagery that counters misinformation or propaganda.
- Provides media outlets with imagery that would otherwise be difficult, if not impossible, to obtain.
- Provides documentation in support of assessment and investigation.
- Provides imagery in support of Public Affairs public and command information efforts, particularly the Army expanding online presence.

For more information on Combat Camera, see FM 3-55.12.

Military Deception
Military deception involves actions executed to deliberately mislead adversary military, paramilitary or violent extremist organization (VEO) decisionmakers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the

friendly mission. Military deception does not fall under the direct purview of the G-7 (S-7) but is considered an enabling capability to Inform and Influence Activities.

Counterdeception contributes to situational understanding by protecting friendly human and automated decisionmaking from adversary deception. Counterdeception's goal is to make Army commanders aware of adversary deception activities so they can formulate informed and coordinated responses.

Deception in Support of Operations Security (DISO). A DISO is a military deception activity that protects friendly operations, personnel, programs, equipment, and other assets against foreign intelligence security services (FISS) collection. The intent of DISO is to create multiple false indicators to confuse or make friendly force intentions harder to interpret by adversary or enemy intelligence gathering apparatus, limiting the ability to collect accurate intelligence on friendly forces.

Tactical deception (TAC-D). TAC-D consists of deception activities planned and conducted to support battles and engagements. TAC-D is planned and executed by, and in support of, tactical-level commanders to cause foreign entity actions that are favorable to the U.S. commanders' objectives. TAC-D is conducted to influence immediate combat operations in order to gain a tactical advantage over an adversary, to mask vulnerabilities in friendly forces, or to enhance the defensive capabilities of friendly forces. TACD is usually "nested" within other operations as part of the JFC's or JTF's Annex C-3-A.

Cyber Electromagnetic Activities

Cyber Electromagnetic Activities seize, retain and exploit advantages in cyberspace and the electromagnetic spectrum, enabling Army forces to retain freedom of action while denying freedom of action to enemies and adversaries.

Cyber Electromagnetic Activities is divided into two lines of effort: the cyberspace operations line of effort and the electronic warfare line of effort. Within these two lines of effort are the six subcomponents: cyber network operations, cyber warfare, electronic attack, electronic protection, and electronic warfare support, and electromagnetic spectrum operations.

Although Inform and Influence Activities and Cyber Electromagnetic Activities are individual staff tasks under the Mission Command warfighting function, integration of Cyber Electromagnetic Activities resides in the Cyber Electromagnetic element of the Mission Command cell and through the Cyber Electromagnetic Activities and Inform and Influence Activities working groups.

Cyber Electromagnetic Activities is able to provide messaging venues and other messaging effects through cyber network operations and electronic warfare attack and support activities to influence enemy target audiences and individuals.

For more information on Electronic Warfare Operations, see FM 3-36. Army Cyber Command and CAC, Capabilities, Development and Integration Directorate (CDID) are currently working on the FM 3-XX, *Cyber Electromagnetic Activities* initial draft (TBP).

Operations Security

Operations security is the process by which the Army protects human and automated decisionmaking in peacetime and in conflict. It is a commander's responsibility. The objective of operations security is to enhance the probability of mission success by preserving the advantages of initiative secrecy and surprise. Operations security is a force multiplier. It includes reducing predictability and eliminating indicators of operations. Operations security countermeasures are used to deny adversary knowledge of friendly operations, requiring him to expend more resources to obtain the critical information needed to make decisions.

Operations security must be considered for all phases of planning and execution. The operations security process will be used to: determine critical information, which must be protected; analyze the adversary's ability to collect intelligence on our forces; and identify vulnerabilities. Commanders will ensure that an operations security process is incorporated into all plans for all phases of the operation. Commanders should use an established operations security process for inclusion into operational planning. Additionally, Operations security countermeasures will be employed to reduce or eliminate vulnerabilities and indicators in order to reduce risk to soldiers (U.S. forces) and operations.

The commander will approve the unit's critical information list (CIL) and ensure that it is circulated to all members of the command. Critical information is the answer to questions regarding essential elements of friendly information. This information is deemed critical because if elements are compromised it would significantly degrade or prevent mission success. Critical information should be disseminated as required to support the mission in a manner that it is accessible to all elements associated with the mission.

For more guidance on Operations Security, see FM 3-37.

Counterintelligence

Counterintelligence serves to deny, degrade, disrupt, or mitigate Foreign Intelligence and Security Services (FISS) and International Terrorism Organizations (ITO) ability and capability to successfully execute intelligence collection targeting U.S. or friendly force interests. Counterintelligence focuses on countering FISS and ITO intelligence collection activities targeting information or material concerning U.S. or friendly force personnel, activities, operations, plans, equipment, facilities, publications, technology, or documents either classified or unclassified. Counterintelligence does this without official consent of designated U.S. release authorities, for any purpose that could cause damage or otherwise adversely impact the interests of national security of the U.S. ability to fulfill national policy and objectives.

Counterintelligence includes all actions taken to detect, identify, track, exploit, and neutralize the multidiscipline intelligence activities of adversaries. It is a key intelligence community contributor to protect U.S. interests and equities. Counterintelligence elements are instrumental in contributing to situational awareness in the area of influence. It may corroborate other intelligence discipline information as well as cue other intelligence assets through its core competencies and counterintelligence technical services.

Within Inform and Influence Activities, the counterintelligence role consists of countering adversarial human intelligence (HUMINT) targeting of U.S. Inform and Influence Activities and providing threat analysis for counter-Signals Intelligence (SIGINT) analysis pertinent to Inform and Influence Activities. Information provided by counterintelligence elements can assist the commander and staff in developing an engagement strategy with the ability to counter, deter, neutralize, exploit, or at least mitigate the adversary's information operations efforts.

For more information on counterintelligence, see FM 2-0.

Civil Military Operations / Civil Affairs Operations

Civil military operations support mission objectives by providing commanders a way to establish, maintain, influence, or exploit relations between military forces, governmental and non-governmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area. Civil military operations typically include infrastructure support activities or human support functions by military forces that are normally the responsibility of local, regional, or national governments. These activities can occur prior to, during, or subsequent to other military operations. Civil military operations may be performed by

designated civil affairs, by other military forces, or by a combination of civil affairs and other forces. (FM 1-02)

Civil Affairs are the designated Active and Reserve Component forces and units organized, trained, and equipped specifically to conduct Civil Affairs activities and to support Civil Military Operations. Often, these Civil Affairs personnel have unique skills: doctors, veterinarians, urban planners, wastewater engineers, etc. They bring these skills, often from civilian job experiences, to the combat zone to help friendly forces handle similar problems with the civilian populace.

The identifying characteristic of Civil Military Operations/Civil Affairs that differentiates it from Inform and Influence Activities is one of purpose, focus and specialization. Civil Military Operations/Civil Affairs is focused squarely and only on the local populace and on the creation of favorable civil considerations in which military operations can occur. In fact, any military operation that involves interaction with the civilian population can be considered Civil Military Operations. By specialization, Civil Affairs forces focus on issues such as infrastructure, governance, agriculture, health and human services and finance. In contrast, Inform and Influence Activities is an integrating function focusing on all audiences influencing the operational environment. It recognizes the power of Civil Military Operations to contribute to the commander's overall inform and influence effort and harmonizes this contribution in with other capabilities, such as Military Information Support Operations, Public Affairs and Soldier and leader engagement. Put another way, all Civil Military Operations inform and influence the local population in some manner, but not all Inform and Influence Activities efforts are Civil Military Operations.

For more information on Civil Affairs Operations, see FM 41-10.

Special Technical Operations

The Integrated Joint Special Technical Operations (IJSTO) process is an option when addressing Inform and Influence Activities problem sets identified by the staff. A staff submits an ISTO request when traditional information-related capabilities will not successfully accomplish the desired end state. The staff will request assistance through established staff channels and procedures for planning. Currently, Special Technical Operations billets exist in Division and higher echelons, in order to support these planning and execution requests and attempt to fill the gap between traditional information-related capabilities and special problem sets. When requesting Integrated Joint Special Technical Operations support, it is important to focus on the problem end state and not specific capabilities or desired effects. Because of the sensitive nature of Special Technical Operations capabilities, the staff needs to keep in mind that Integrated Joint Special Technical Operations support is a complicated and thorough process. The Integrated Joint Special Technical Operations process involves many agencies to develop the concept of operations and acquire authorization and typically requires an average of ninety days. Unless concepts and authorizations are already established, staffs of Integrated Joint Special Technical Operations should not typically consider such requests for time-sensitive event planning.

Commander designated Capabilities (other)

Commander designated capabilities (other) are determined during the operations process. The operations process aids the commander and staff to decide what other capabilities, not specified as an information-related capability, could be used to support, inform, and/or influence lines of effort.

The Commander's Role

The operational environment yields a high and often decisive impact to the side which best leverages the information environment. Success requires commanders to focus attention to inform and influence activities throughout operations. Commanders incorporate cultural

awareness, relevant social and political factors, and other informational aspects related to the mission in their understanding and visualization of the end state and throughout operational design. Commanders clarify effects they intend to achieve through their guidance and intent. Commanders ensure the IIA officer and staff identify those relevant audiences and actors, and then integrate and synchronize themes, messages and actions to achieve the desired perceptual or behavioral effects for each. Finally, commanders understand the advantages of building partner capacity in this critical mission area, through their promotion of informational activity and capability by, with, and through host-nation forces.

Updated: October 2011

This Page Intentionally Blank

Marine Corps Information Operations Doctrine

At the time this primer was released, several key USMC IO documents were under review, revision or development; Marine Corps Order 3120.10A Marine Corps Information Operations Program, Marine Corps Warfighting Publication 3-40.4 MAGTF IO, and the USMC IO Concept of Operations. All documents are projected to be signed during FY 2012.

Key documents:

- Marine Corps Order 3120.10, Marine Corps Information Operations Program (MCIOP), 30 June 2008.
- Marine Corps Information Operations Center: Concept of Operations for Information Operations Support to the Marine Air-Ground Task Force, 19 June 09.

Key doctrinal documents:

- MCWP 3-40.4, *MAGTF Information Operations*, 9 Jul 2003.
- MCWP 3-40.6, *Psychological Operations*, April 2005. (Beginning revision in Nov 2011)
- Other documents:
  - Marine Corps Order 3432.1, THE MARINE CORPS OPERATIONS SECURITY (OPSEC) PROGRAM
  - Marine Corps Bulletin 5400, CH1, CMC Washington DC CDI/TFSD 122025Z AUG 11, Activation of the MARCOR Information Operations Center (MCIOC) Phase Two and Three.

Fundamental changes in the global environment have created conditions in which the traditional military activity of Information Operations (IO) will serve a critical role in achieving operational and tactical level objectives that have potential to impact our military strategy and national security objectives. The Marine Corps IO Program (MCIOP) will build the Marine Corps' capability and capacity to plan, execute and access IO in order to create an operational advantage for the commander by affecting relevant target audiences. Tasks outlined in the MCIOP support a desired end state that IO will be an essential part of routine operations in the expeditionary and joint environments. IO actions will be integrated and synchronized across the Marine Air-Ground Task Force (MAGTF) Command Element (CE), MAGTF Major Subordinate Elements (MSEs), other USMC discreet capabilities (Fires, EW, Cyber, etc.), as well as higher and adjacent headquarters.

Principles:

- *IO is an integral function of the MAGTF.*
- *MAGTF IO is focused on the objective.*
- *The MAGTF commander's intent and concept of operations determine target audiences and objectives.*
- *MAGTF IO must be synchronized and integrated with those of the higher and adjacent commands*
- *MAGTF IO is supported by the total force.*
- *A coherent IO concept of operations integrates all of the MAGTF's capabilities and activities.*
- *Intelligence support is critical to the planning, execution, and assessment of IO.*

Information Operations in Support of the Expeditionary "Middle-weight" Force:
Marine Corps IO support maneuver warfare through the integration, coordination, and synchronization of all actions taken in the information environment to affect a target audience's behavior in order to create an operational advantage for the commander. Information operations enhance the ability of the MAGTF to project power during peace and war. They complement and facilitate the traditional use of military force and, in some instances, may obviate the need for application of kinetic capability if synchronized correctly. IO supports the integration of situational awareness, operational tempo, influence, and power projection to achieve advantage.

IO is a critical integrating function that augments the warfighting functions of command and control (C2), fires, maneuver, logistics, intelligence, and force protection. IO is not simply another "arrow" in the MAGTF commander's quiver; it is an overarching philosophy that "makes the bow stronger." Current DOD and USMC doctrine expands the traditional list of information-related capabilities to include any and all MAGTF capabilities that have effects in the physical, information and cognitive dimensions of the information environment. IO conducted by MAGTFs support battle space shaping, force enhancement, and force protection activities.

MAGTFs will execute IO to enable and enhance their ability to conduct military operations consistent with the Marine Corps' capstone concept, *Expeditionary Maneuver Warfare (EMW)*. Future development and integration of IO in the USMC will focus on integrating discreet capabilities in an amphibious and austere environment to achieve the commander's desired end state. IO capability will also be shaped to allow the MAGTF access to national level resources and other service components when necessary.

IO can increase strategic agility by utilizing the reach back capability via MAGTF and Amphibious C4I systems, thus allowing the MAGTF to draw upon information sources outside its area of operations. IO can extend operational reach through informational and media activities that unify power projection with influence projection. IO can increase tactical flexibility by providing the MAGTF commander with a range of both lethal and nonlethal options. Finally, IO can enhance support and sustainment by enabling power projection against distant targets without increasing the MAGTF's footprint ashore.

Staff Responsibilities:

- The G-3/S-3 is responsible for IO. The future operations (FuOps) section in conjunction with the MAGTF Fires and Effects cell is responsible for overseeing the planning and coordination of the IO effort. The MAGTF IO officer, within G-3/S-3 FuOps is responsible for:
  - The broad integration and synchronization of IO efforts.
  - Responding directly to the G-3/S-3 for MAGTF IO.

- Participating, as a member, in the operational planning team (OPT) during all phases of planning to ensure coordinated operations.
- Preparing the IO appendix to the operation order (OPORD).
- Directing the efforts of core IO cell personnel as well as liaisons from external agencies.
- Ensuring that all IO matters are coordinated within the MAGTF staff, higher headquarters, and external agencies.
- Coordinating and supporting IO activities of subordinate commands.
- Providing direct input to both the targeting and intelligence cycles established by the staff.

Information Operations Cell:
The IO cell is a task-organized group, established within a MAGTF and/or higher headquarters to integrate information-related capabilities. A fully functioning IO cell will plan for, monitor the execution of, and assess the effects of IO across all MAGTF operations. The cell will accomplish this through extensive planning and coordination among all the elements of the staff (i.e.: IO working group). The size, structure and placement of the IO cell within the staff are tailored to meet the mission and commander's intent.

Intelligence and Information Operations:
Integration of intelligence into the Information Operations Cell is critical to the planning, execution, and assessment of IO. This critical integration must begin at the earliest stage of the planning effort. Information operations planners must understand that limited intelligence resources, legal constraints, long lead times, and the dynamic nature of the information environment have an effect on integration timelines. Successful execution of IO requires an in-depth understanding of the information environment (physical, information and cognitive dimensions) as well as socio-cultural awareness of the operating environment. The intelligence needed to affect adversary or other target audience decisions often requires specific sources and methods to be positioned and employed over a long period of time to collect and analyze the needed information. In order to effectively engage the intelligence system, the IO staff should clearly articulate intelligence requirements so that the G-2/S-2 staff can effectively work on behalf of the IO staff. The IO staff should establish relationships with the G-2/S-2 staff that will facilitate successful IO planning and execution initiatives.

Information-related Capabilities:
IO is an integrating function across the entire MAGTF capability set. Some of the elements of IO are more offensive, defensive or informational in nature, but it is their integration into the overall concept of operations that ensures successful employment of IO in support of the MAGTF. USMC IO doctrine does not seek to "own" each capability, instead it seeks to integrate and coordinate each of the capabilities when their synchronized effects provide an operational advantage.

Summary:
MAGTF Commanders and Marines naturally understand IO are important in today's operating environment and are frequently aware of the second- and third-order effects of their actions and the perceived messages those actions may convey. It is the goal of the MCIOP to enhance this understanding with knowledge; to support MAGTF commanders and Marines on the ground with the appropriate personnel, equipment and resources; and to *integrate* and synchronize Marine actions, information and communications to accomplish the MAGTF mission.

For more information contact Mr. James McNeive at 703-784-5826 (DSN: 273) or email at jmcneive@mcia.osis.gov.

Updated: October 2011

This Page Intentionally Blank

Navy Information Operations Doctrine

Key doctrine and tactics, techniques, and procedures

- NWP 3-13, *Navy Information Operations*, June 2003 (in revision)
- NTTP 3-13.1, Theater and Campaign Information Operations Planning, April 2008
- NTTP 3-13.2, *Navy IO Warfare Commander's Manual*, May 2006 (in revision)
- Other key TTP:
  - NTTP 3-51.1, Navy Electronic Warfare (Feb 06)
  - NWP 3-53, Navy Psychological Operations
  - NTTP 3-54/MCWP 3-40-9, *Operations Security*, Mar 09
  - NTTP 3-58.1, Multi-Service Military Deception Planners Guide (April 2007)
  - NTTP 3-58.2, *Navy Military Deception*, April 2009
  - NTTP 3-51.2, Multi-Service Reprogramming at Sea of Electronic Warfare and Target Sensing Systems, January 2007 (in revision)
  - NWP 3-63, Navy Computer Network Operations Vol 1 (April 2008)
  - NWP 3-63, Navy Computer Network Operations Vol 2 (Sep 2008)
  - NTTP 3-13.6, Countering Counter Intelligence, Surveillance, Reconnaissance, Targeting (in development)
  - NTTP 3-51.3, Communications Electronic Attack (in development)
  - TM 3-01.1-07, Integrated HardKill and Softkill Tactics in Antiship Missile Defense
  - NTTP 2-02.1, Strike Group and Unit Level Cryptologic Operations
- **NWPs, NTTPs, TACMEMOs, and CONOPS are available at** the Navy Doctrine Library System link: http://www.nwdc.navy.smil.mil

Summary of Navy Information Operations Doctrine and Concepts

- NWP 3-13 Navy Information Operations is in revision.
- The effects of the establishment of USCYBERCOM and the supporting FLEET CYBER COMMAND are not currently reflected in Navy IO TTP and CONOPS and are not addressed in this summary.
- When NWP 3-13 is completed the new document can be found at the Navy Doctrine Library System link: http://www.nwdc.navy.smil.mil.

Introduction

The United States has experienced a shift from strictly symmetric, or force-on-force, warfare to more asymmetric warfare and military operations. Many of today's adversaries rely primarily on operations such as terrorism, disinformation, and propaganda campaigns to circumvent or undermine U.S. and allied strengths and exploit friendly vulnerabilities. Future Navy forces will continue to face adversaries outside the generally accepted force-on-force environment of the past. Naval forces are challenged by asymmetric operations in all domains—surface, subsurface, air, ground, and cyberspace—and must therefore defend against, defeat, deny, or negate the capabilities that will be used to prevent U.S. freedom of access. Information

Operations (IO) is applicable across the range of military operations, (e.g., supporting major combat operations, global war on terrorism, etc.), in support of the Navy operating concept. Furthermore, the Navy must provide IO capabilities, organizational structures, planning processes, and personnel to maritime headquarters (MHQs)/joint force maritime component commanders (JFMCCs) engaged in theater security cooperation plans (TSCPs) and/or combat operations that enable our forces to engage in the asymmetric domain. Rapid advances in information technology provide today's military with unparalleled abilities to collect, process, and disseminate information. Technological advances have also increased the commander's vulnerability as a target for adversary information collection, shaping, and attack. IO will continue to play a key role by allowing the Navy and its partners to dominate warfare in the maritime domain. Operations within this domain include controlling the sea, conducting operational maneuvers throughout the world, deterring aggression through forward presence and influence operations in peacetime, responding to crisis, conducting major combat operations, and complementing other instruments of national power by projecting power from the sea, directly and decisively influencing events ashore.

Core Capabilities of Information Operations

IO was established as a warfare area within the Navy with the goal of affecting accuracy, usability, timeliness, completeness, or relevance of information used in guiding and conducting operations. IO includes electronic warfare (EW), computer network operations (CNO), military information support operations (MISO), military deception (MILDEC), and operations security (OPSEC). Supporting capabilities of IO include physical attack, physical security, information assurance, public affairs (PA), combat camera/visual information, civil-military operations, legal affairs, meteorology, intelligence, and oceanography. This is Navy IO at its most fundamental level and could consist of a wide (almost unbounded) array of "weapons," within the core, supporting, and related capabilities above.

IO is an integral part of the Navy planning and targeting process that continues through the range of military operations (see Figure 1). From guiding effects-based planning in the earliest stages to the weaponeering assessment phase of the targeting cycle, IO planners can assist in determining the right mix of maneuver, and kinetic/nonkinetic weapons that will produce the commander's desired effect. In addition to offering nonkinetic options to traditional strike warfare, IO plans often require the use of strike group maneuvers (concentration of forces and presence), kinetic strikes, and special operations warfare to deny, disrupt, destroy, or degrade information systems to attain overall campaign objectives. While each capability of IO includes a specialized planning process and can be applied to military operations individually, their coordinated application maximizes friendly advantages.

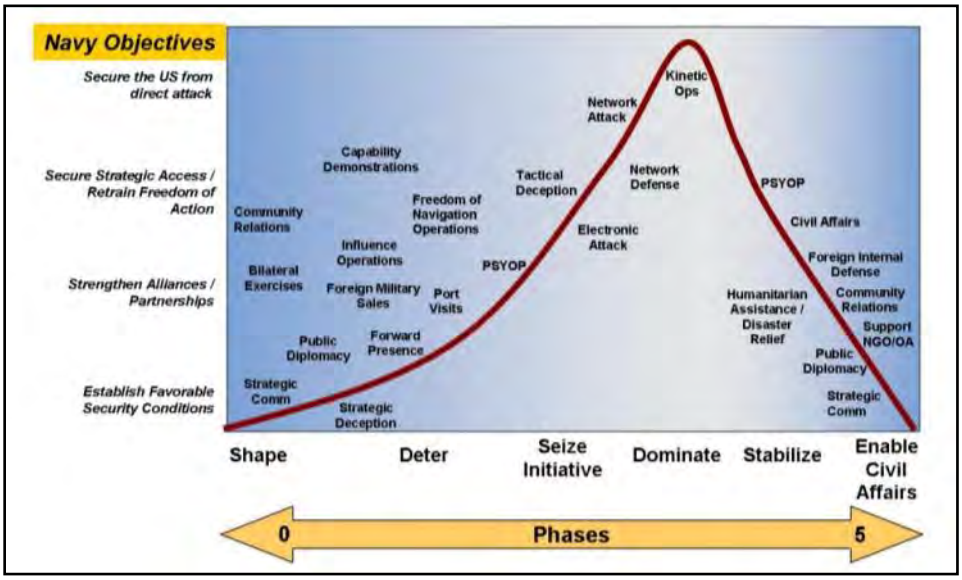


Figure 1. Range of Military Operations Integrating IO

Information Superiority

Information superiority embodies the ability to collect, process, and disseminate the correct information to the right person, at the right place and time, in the right form, while denying an adversary the ability to do the same. Network-centric operations can foster information superiority by networking sensors, decisionmakers, and shooters. The goal of using network-centric operations is to increase mission effectiveness in order to achieve an increased state of readiness.

This superiority contributes to the ability to project maritime power forward from the sea and ultimately in all warfighting domains. IO supports information superiority by corrupting, deceiving, delaying, denying, disrupting, degrading, or destroying one of the dimensions of information before it is presented to the adversary's commander, while protecting the same friendly information dimensions. Enabled through FORCENet (discussed later), information superiority is achieved through effects-based approach to operations, maritime power projection, maritime influence, target development, and environmental awareness and shaping (EAS). All echelons and warfare areas strive for and plan to achieve and maintain information superiority through coordinated efforts among the operations, intelligence, and command, control, communications, and computers (C4), and knowledge management.

Effects-Based Approach to Operations

An effects based approach to operations focuses on improving the commander's ability to affect an adversary's behavior and/or capabilities through the integrated application of select instruments of national power (diplomatic, information, military, economic). Effects are created to achieve objectives and are characterized as the physical and/or behavioral state of political, military, economic, social infrastructure, and information systems. An effects-based approach seeks to develop a commonly shared understanding of the operational environment to provide the commander with a more comprehensive picture of the challenges and the best balance of capabilities to shape the environment. The three main elements within an effects-based approach to operations are as follows:

1. Visualizing the operational environment beyond the traditional military battlespace as an interconnected system-of-systems comprised of friends, adversaries, and the unaligned.
2. Integrating military actions with those of other instruments of national power.
3. Assessing system behaviors and capabilities and effects attainment in addition to task accomplishment.

Maritime Power Projection

No one can predict with certainty the future security environment, but emerging trends require that the Navy focus on littorals and the land beyond. The Navy must remain expeditionary in nature, controlling the sea and moving around the globe to support U.S. national interests. The vision for the future is a Navy and Marine Corps team that will maintain a robust and credible forward presence. These forces provide a framework that complements other instruments of national power to build stability and favorably shape areas overseas. Forward presence, combined with knowledge superiority within the environment, will achieve the ultimate objective—maritime power projection—projecting U.S. power and influence from the sea, directly and decisively influencing events ashore.

Maritime Influence

Naval forces deployed or stationed in areas overseas demonstrate our national resolve, strengthen alliances, and dissuade potential adversaries. IO provides significant support to maritime influence operations during the phases of planning and assessment. U.S. naval forces will protect and use information to influence adversaries, advance friendly objectives, and shape the operating environment to our advantage. With an effects based approach to operations, maritime influence coordinates the employment of maritime activities to affect the attitudes and behaviors of an intended audience in support of commander objectives. With the goal of advancing U.S. interests, maritime influence activities may include actions to deter adversaries, reassuring allies and friends, sending signals of U.S. interest, and fostering good will.

Target Development

Warfighters win engagements and wars when the adversary makes a decision—based on knowledge derived from true or perceived information—to surrender due to an inability to obtain desired objectives. A comprehensive assessment of the adversaries and friendly abilities and functions within the operational environment provide the first step into developing targets. Friendly forces design all campaign plans to influence the adversary to make such a decision. The people and systems that comprise the information grids filter and process the information upon which the commander bases decisions and therefore require defending as part of IO planning. Target development includes nodes that have an impact on the adversary decision making process, which may include command and control systems, communications and weapon systems, and other situation awareness tools.

Environment Awareness and Shaping

EAS describes the functions performed by organizations to ensure that, despite the wide range of nonlethal and lethal means at the disposal of adversaries or potential adversaries, friendly forces are consistently capable of conducting decisive operations and achieving desired results at a minimal loss to friendly forces. The commander uses EAS to identify, protect, and leverage critical information systems, emissions, transmissions, and operational indicators, to achieve and maintain information superiority. Environment awareness equates to knowledge of the operational environment. This knowledge, resulting from the fusion of key elements of information, allows the commander and staff to correctly anticipate future conditions, assess changing conditions, establish requirements and priorities, and exploit emerging opportunities, while mitigating the impact of unexpected adversary actions. Environment shaping is the conscious action of molding the environment to prevent conflicts or placing U.S. interests in a favorable position. It involves the continual process of developing, evaluating, and revising the

force operational profile within the environment, providing all warfare commanders with critical planning and execution support to ensure that missions are conducted with the least risk to friendly assets.

Navy Information Operations Employment Concept

Sea Power 21 describes future naval operations that will use information superiority and dispersed, networked force capabilities to deliver effective offensive power, defensive assurance, and operational independence to joint force commanders. To support Sea Power 21, the Navy's focus is to integrate and align IO to support all levels of operations:

At the strategic level, national leadership and regional commanders will use IO to achieve national/theater shaping and influencing objectives. Regional commanders will integrate Navy IO capabilities with other services, other U.S. government departments and agencies, and partner nations as part of their theater security cooperation plans (TSCP).

At the operational level, IO supports campaign/major operational objectives by providing information superiority through shaping and controlling the information environment. At this level, the focus of IO is control of adversary lines of communication (logistics information, command and control, and related capabilities and activities) while protecting the friendly information environment.

At the tactical level, Navy IO will make full use of the core capabilities to dominate the information environment for the commander. At this level, IO will be used to tactically influence adversaries or deny, destroy, or degrade systems critical to the adversary's conduct of operations.

The following key organizational concepts are being implemented to affect the operational model summarized in Figure 2:

- **Maritime Headquarters IO Cell**

  References: NTTP 3-32.1 Maritime Headquarters with Maritime Operations Center, NTTP 3-13.1 Theater and Campaign Information Operations Planning (April 2008)

  The MHQ IO Cell contributes to the shaping of the environment to enable tactical units to successfully execute assigned tasks. The IO Cell coordinates with the other maritime headquarters staff cells (i.e. horizontally) and with the IO cells of the other components and other government agencies through the joint force commander's IO staff (i.e. vertically). The IO cell works with elements of both the current operations cell, the future operations (FOPS) cell, and the Plans cell. Emphasis has been placed on the flexibility and scalability of Navy maritime headquarters (MHQs) with maritime operations centers (MOC) designed to perform normal and routine operations. Fleet commanders will establish global MHQ-MOC's to serve geographic areas of responsibility and may have additional JFMCC responsibilities.

  The MHQ-MOC performs the fleet management and command and control (C2) role at the Navy operational-level of command across the range of military operations (ROMO). More importantly, the MHQ-MOC performs the roles of planning, directing, monitoring and assessing the integration and synchronization of Joint Maritime Force operational missions as outlined in the Navy operating concept. The MHQ-MOC organizes staff roles and responsibilities by integrating warfighting functions (C2, intelligence, movement and maneuver, fires, sustainment, and protection) across staff functions. Thus, the assessment and long-range planning functions are joined in a future plans center and short term planning is performed in the future operations and current operations cells of the operations center. A MHQ-MOC is able to integrate staff actions horizontally and vertically, simultaneously conducting service and joint operations through the MOC and the fleet management functions by leveraging specialized fleet management staff elements. The MHQ-MOC has the capability to fulfill various roles including Commander, Joint Task Force

(CJTF), Joint Force Maritime component commander (JFMCC), and naval component commander (NCC). Both the MOC and fleet management elements of the staff are supported by a third component consisting of shared support elements that provide personnel, processes, and systems that affect operations and fleet management functions.

- **Strike Group Level - The IO Warfare Commander (IWC)**

The IO Warfare Commander (IWC) assigned to each strike group is responsible for the protection of assigned forces against hostile information, information systems, and electronic attacks, as well as hostile propaganda and deceptive techniques. The IWC maintains the tactical IO picture and is responsible to the force commander for establishing force posture for emissions control (EMCON), information conditions (INFOCON), spectrum management, and maintaining a favorable tactical situation (TACSIT). The IWC supports all force plans and evolutions, while coordinating with theater and joint task force (JTF) IO planners.

Levels of Operations	Key Goals Include…	Objectives to Support Goals Include…	Application of Navy IO Include…	Impact of Navy IO…
Strategic (National and Theater) National Security Strategy National Guidance & Military Strategy Theater Strategy & Campaign Plans	Implementation of long-term national and theater shaping, and theater security cooperation plans (TSCPs).	Influence nations/potential adversaries/decision makers globally or in a specific region(s). Support diplomacy, stabilize regions, and assure allies. Deter war. Support intelligence preparation of the environment, and shape environment to U.S. advantage.	CCDR, MHQ, and JFMCC (when assigned), will use IO to support TSCPs through presence, coordination with public affairs, port calls, multination exercises, peace operations, and support to strategic communications.	Demonstrate that the U.S. is engaged in the region and can project power. Demonstrate that the U.S. military can project power anywhere in region. Prepare intelligence baseline for future ops. Shape positive perception of U.S. actions.
Operational Subordinate Campaign Plans Major Operations	Decisively defeat adversary ability to control forces.	Shape and control information environment. Use spectrum of IO core capabilities to conduct (or support) force application, deny adversary intelligence, surveillance, reconnaissance (ISR) and command, control, communications, computers (C4). Support information superiority. Protect friendly information environment and physical domain.	The / MHQ use IO in continuing strategic roles plus applying Navy IO capabilities and weapons to engage adversary C4 and ISR and MISO to influence adversary forces and populations. Directly support conduct of joint or maritime operations/power projection.	Support information superiority for the joint force commander. Control information environment and physical domain by influencing, disrupting, or corrupting adversarial human and automated decisionmaking.
Tactical Operational Orders and OPTASKS Battles Engagements	Strike Group commander effectively using forces to achieve commander's assigned tasks. Coordinated use of EW, MISO, MILDEC, CNO, OPSEC capabilities embedded in Navy forces.	Control tactical information environment and physical domain. Disrupt adversary operations. Undermine adversary ability and will to fight. Disrupt adversary C4, ISR and defensive systems. Protect the naval/joint battle force.	During initial phases of a campaign, Navy strike groups may have the preponderance of tactical IO assets. Strike Group commander via the IO warfare commander will use IO to support MHQ objectives, and other tactical operations.	Achieve/maintain decision superiority, control tactical information environment and physical domains, achieves operational objectives of the MHQ and tactical objectives of the strike group commander.

Figure 2. Operational Model

Air Force Information Operations Doctrine

Key doctrinal documents:

AFDD 3-12, *Cyberspace Operations*, 15 July 2010
AFDD 3-13, *Information Operations*, 11 January 2005
AFDD 3-13.1, *Electronic Warfare Operations*, 5 November 2002
AFDD 3-61, *Public Affairs Operations*, 23 December 2010

AFDDs are available at: http://www.e-publishing.af.mil/.

Information below is valid as of September 2011. However, at the time of printing the Information Operations Primer for AY12, Air Force doctrine documents are being revised, which may result in some changes to Air Force Information Operations doctrine. This section reflects the currently published doctrine.

Excerpts of Air Force Doctrine - AFDD 3-13

Forward

The Air Force recognizes the importance of gaining a superior information advantage—an advantage obtained through information operations (IO) fully integrated with air, space, and cyberspace operations. Today, gaining and maintaining information superiority are critical tasks for commanders and vital elements of fully integrated kinetic and nonkinetic effects-based operations. Information operations are conducted across the range of military operations, from peace to war to reconstitution. To achieve information superiority, our understanding and practice of information operations have undergone a doctrinal evolution that streamlines the focus of IO to improve the focus on warfighting.

The framework of information operations groups the capabilities of influence operations, electronic warfare operations, and network warfare operations according to effects achieved at the operational level. Each of these capabilities are separate and distinct capabilities that, when combined and integrated, can achieve effects greater than any single capability. Integrated Control Enablers (ICE) is a term used to define what was formerly expressed as information-in-warfare, or IIW. As our understanding of IO has advanced, we have come see that ICE are not IO, but rather the "gain and exploit" capabilities that are critical to all air, space, and information operations. This framework reflects the interactive relationship found between the defend/attack and the gain/exploit capabilities in today's Air Force.

Foundational Doctrine Statements
Foundational doctrine statements are the basic principles and beliefs upon which AFDDs are built.

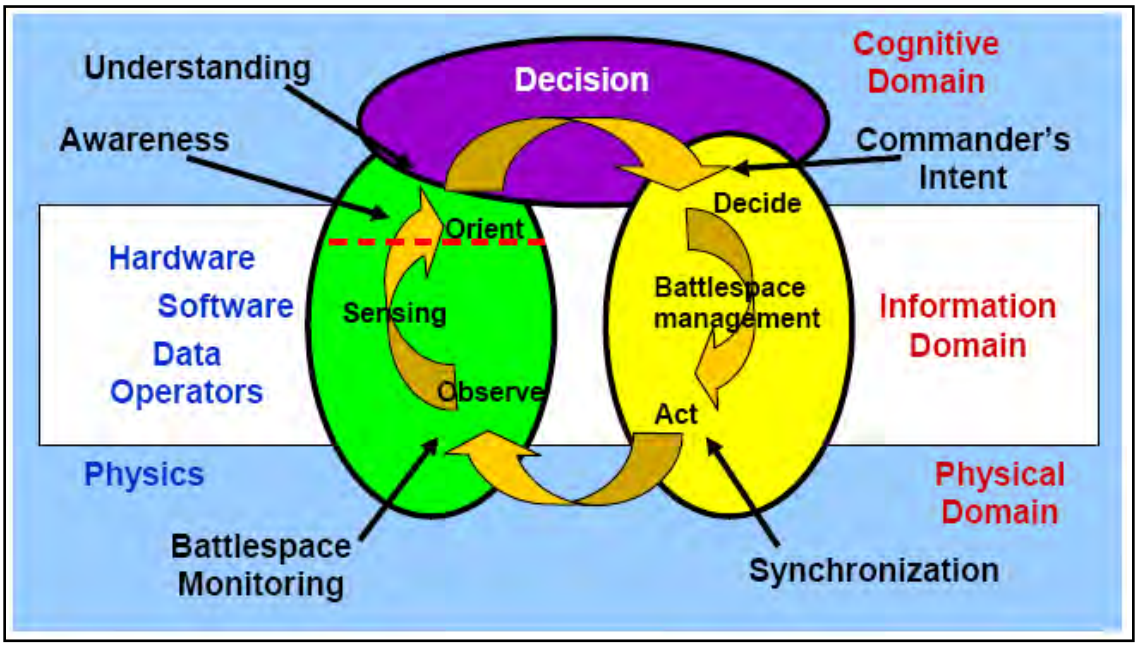
- Information operations (IO) are integral to all Air Force operations and may support, or be supported by, air, space, and cyberspace operations.
- The thorough integration of kinetic and nonkinetic air, space, and information capabilities provides the Air Force with a comprehensive set of tools to meet military threats.
- The Air Force defines information superiority as the degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition.
- Decision superiority is about improving our capability to observe, orient, decide, and act (OODA loop) faster and more effectively than the adversary. Decision superiority is a relationship between adversary and friendly OODA loop processes.
- The three IO capabilities—influence operations, electronic warfare operations, and network warfare operations—while separate and distinct, when linked, can achieve operationally important IO effects. Effective IO depends on current, accurate, and specialized integrated control enablers (ICE) to provide information from all available sources.
- Information operations conducted at the operational and tactical levels may be capable of creating effects at the strategic level and may require coordination with other national agencies.
- IO should be seamlessly integrated with the normal campaign planning and execution process. There may be campaign plans that rely primarily on the capabilities and effects an IO strategy can provide, but there should not be a separate IO campaign plan.
- IO applications span the spectrum of warfare with many of the IO capabilities applied outside of traditional conflict. IO may offer the greatest leverage in peace, pre-conflict, transition-to-conflict, and reconstitution.
- Air Force IO may be employed in non-crisis support or military operations such as humanitarian relief operations (HUMRO), noncombatant evacuation operations (NEO), or counterdrug support missions where Air Force elements are subject to asymmetric threats that could hinder operations or place forces at risk.
- IO presents additional challenges in effects-based planning as there are many variables. Many of these variables have human dimensions that are difficult to measure, may not be directly observable, and may also be difficult to acquire feedback.

1 – The Nature of Information Operations

General Information operations are the integrated employment of the capabilities of influence operations, electronic warfare operations, and network warfare operations, in concert with specified integrated control enablers, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own. Information operations provide predominantly nonkinetic capabilities to the warfighter. These capabilities can create effects across the entire battlespace and are conducted across the spectrum of conflict from peace to war and back to peace. Information superiority is a degree of dominance in the information domain, which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition. Information superiority is a critical part of air, space, and cyberspace superiority, which gives the commander freedom from attack, freedom to maneuver, and freedom to attack. Information operations are integral to all Air Force operations and may support, or be supported by, air, space, and cyberspace operations. IO, therefore, must be integrated into air, space, and cyberspace component operations in the same manner as traditional air, space, and cyberspace capabilities.

Warfare in the Information Age Warfare in the information age has placed greater emphasis on influencing political and military leaders, as well as populations, to resolve conflict. Information technology (IT) has increased access to the means to directly influence the populations and its leaders. IT has distributed the process of collection, storage, dissemination, and processing of information. The Air Force goal is to leverage this technology to achieve air, space, cyberspace, and information superiority and to be able to operate in a faster decision cycle (decision superiority) than the adversary. Decision superiority is a competitive advantage, enabled by an ongoing situational awareness, that allows commanders and their forces to make better-informed decisions and implement them faster than their adversaries can react. Decision superiority is about improving our ability to observe, orient, decide, and act (OODA loop) faster and more effectively than the adversary. *Joint Vision 2020* describes it as "better decisions arrived at and implemented faster than an opponent can react, or in a non-combat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission." Decision superiority is a relationship between adversary and friendly OODA loop processes. Decision superiority is more likely to be achieved if we plan and protect our OODA loop processes in conjunction with analyzing, influencing, and attacking the adversary's.

The Information Environment [The information environment can be modeled as the interaction of the physical, information, and cognitive domains as shown below.]



This model provides a means to understand the IO environment. It also provides a logical foundation for the IO capabilities of influence operations, network warfare operations, and electronic warfare operations. All activities in the physical environment have effects in the cognitive environment. Electronic warfare operates in the electromagnetic spectrum, although it creates effects across the range of the IO operating environment. Network warfare operations are focused on the information domain, which is composed of a dynamic combination of hardware, software, data, and human components. Influence operations are focused on affecting the perceptions and behaviors of leaders, groups, or entire populations. The means of influencing can be physical, informational, or both. The cognitive domain is composed of separate minds and personalities and is influenced by societal norms, thus the cognitive domain is neither homogeneous nor continuous.

Societies and militaries are striving to network this "information domain" with the objective of shortening the time it takes for this distributed observe, orient, decide, and act process to occur. It also allows us to automate certain decision processes and to build multiple decision models operating simultaneously. In essence, the information domain continues to expand. New technology increases our society's ability to transfer information as well as an adversary's opportunity to affect that information. Information operations are not focused on making decision loops work; IO focuses on defending our decision loops and influencing or affecting the adversary's decisions loops. This integration of influence, network warfare, and electronic warfare operations to create effects on OODA loops is the unifying theme of IO. Whether the target is national leadership, military C2, or an automated industrial process, how the OODA process is implemented provides both opportunities and vulnerabilities.

The three IO capabilities—influence operations, electronic warfare operations, and network warfare operations—while separate and distinct, when linked, can achieve operationally important IO effects. In addition, effective IO depends on current, accurate, and specialized integrated control enablers (ICE) to provide information from all available sources. The thorough integration of kinetic and nonkinetic air, space, cyberspace, and information capabilities provides the Air Force with a comprehensive set of tools to meet military threats.

Influence Operations Influence operations are focused on affecting the perceptions and behaviors of leaders, groups, or entire populations. Influence operations employ capabilities to affect behaviors, protect operations, communicate commander's intent, and project accurate information to achieve desired effects across the cognitive domain. These effects should result in differing behavior or a change in the adversary's decision cycle, which aligns with the commander's objectives. The military capabilities of influence operations are military information support operations (MISO), military deception (MILDEC), operations security (OPSEC), counterintelligence (CI) operations, counterpropaganda operations and public affairs (PA) operations. Public affairs, while a component of influence operations, is predicated on its ability to project truthful information to a variety of audiences.

Network Warfare Operations Network warfare operations are the integrated planning, employment, and assessment of military capabilities to achieve desired effects across the interconnected analog and digital network portion of the battlespace. Network warfare operations are conducted in the information domain through the combination of hardware, software, data, and human interaction. Networks in this context are defined as any collection of systems transmitting information. Examples include, but are not limited to, radio nets, satellite links, tactical digital information links (TADIL), telemetry, digital track files, telecommunications, and wireless communications networks and systems. The operational activities of network warfare operations are network attack (NetA), network defense (NetD) and network warfare support (NS).

Electronic Warfare Operations Electronic warfare operations are the integrated planning, employment, and assessment of military capabilities to achieve desired effects across the electromagnetic domain in support of operational objectives. Electronic warfare operates across the electromagnetic spectrum, including radio, visible, infrared, microwave, directed energy, and all other frequencies. It is responsible for coordination and deconfliction of all friendly uses of the spectrum (air, land, sea, and space) as well as attacking and denying enemy uses. For this reason it is an historically important coordinating element in all operations, especially as current and future friendly uses of the electromagnetic spectrum multiply. The military capabilities of electronic warfare operations are electronic attack, electronic protection, and electronic warfare support.

Integrated Control Enablers Information operations, like air, space, and cyberspace operations, are reliant on the integrated control enablers (ICE). ICE includes intelligence, surveillance, and reconnaissance (ISR), network operations (NetOps), predictive battlespace awareness (PBA), and precision navigation and timing (PNT). Information operations are highly dynamic and maneuverable. The transition between the find, fix, track, target, engage, and assess (F2T2EA) phases can be nearly instantaneous. The ICE components support this interactive relationship and strive to provide commanders continuous decision-quality information to successfully employ information operations.

2 – Influence Operations

General Influence operations are employment of capabilities to affect behaviors, protect operations, communicate commander's intent, and project accurate information to achieve desired effects across the cognitive domain. They should influence adversary decision-making, communicate the military perspective, manage perceptions, and promote behaviors conducive to friendly objectives. This is accomplished by conveying selected information and indicators to target audiences; shaping the perceptions of target decision-makers; securing critical friendly information; protecting against espionage, sabotage, and other intelligence gathering activities; and communicating unclassified information about friendly activities to the global audience.

Military Information Support Operations Focused on the cognitive domain of the battlespace, MISO targets the mind of the adversary. In general, MISO seeks to induce, influence, or reinforce the perceptions, attitudes, reasoning, and behavior of foreign leaders, groups, and organizations in a manner favorable to friendly national and military objectives. MISO supports these objectives through the calculated use of air, space, cyberspace, and IO with special emphasis on psychological effects-based targeting.

Military Deception Military deception capabilities are a powerful tool in military operations and should be considered throughout the operational planning process. Military deception misleads or manages the perception of adversaries, causing them to act in accordance with friendly objectives.

Operations Security Operations security is an activity that helps prevent our adversaries from gaining and exploiting critical information. OPSEC is not a collection of specific rules and instructions that can be applied to every operation; it is a methodology that can be applied to any operation or activity for the purpose of denying critical information to the adversary. Critical information consists of information and indicators that are sensitive, but unclassified. OPSEC aims to identify any unclassified activity or information that, when analyzed with other activities and information, can reveal protected and important friendly operations, information, or activities.

Counterintelligence The Air Force Office of Special Investigations (AFOSI) initiates, conducts, and/or oversees all Air Force counterintelligence investigations, activities, operations, collections, and other related CI capabilities. Counterintelligence is defined as information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. AFOSI supports influence operations through CI operations designed to detect, destroy, neutralize, exploit, or prevent espionage activities through identification, manipulation, deception, or repression of the adversary.

Public Affairs Operations Commanders conduct PA operations to assess the information environment in areas such as public opinion and to recognize political, social, and cultural shifts. Public affairs operations are a key component of informational flexible deterrent options and

build commanders' predictive awareness of the international public information environment and the means to use information to take offensive and preemptive defensive actions in Air Force operations. Public affairs operations are the lead activity and the first line of defense against adversary propaganda and disinformation. Falsehoods are easily identified when the truth is well known. [Public affairs operations are accomplished through] four core tasks: media operations, internal information, community relations, and strategic communication planning.

Counterpropaganda Operations The Air Force defines counterpropaganda operations as activities to identify and counter adversary propaganda and expose adversary attempts to influence friendly populations and military forces situational understanding. They involve those efforts to negate, neutralize, diminish the effects of, or gain an advantage from foreign psychological operations or propaganda efforts.

Supporting Activities Influence operations are most successful through the seamless integration of kinetic and nonkinetic capabilities. Influence operations may be supported and enhanced by physical attack to create or alter adversary perceptions. Influence operations require support from many Air Force capabilities to include tailored ISR, combat camera operations, and cultural expertise.

3 – Network Warfare Operations

Network warfare operations (NW Ops) are the integration of the military capabilities of network attack (NetA), network defense (NetD), and network warfare support (NS). The integrated planning and employment of network warfare operations along with electronic warfare operations (EW Ops), influence operations, and other military capabilities are conducted to achieve desired effects across the information domain.

Network Attack Network attack (NetA) is employment of network-based capabilities to destroy, disrupt, corrupt, or usurp information resident in or transiting through networks. Networks include telephony and data services networks. Additionally, NetA can be used to deny, delay, or degrade information resident in networks, processes dependent on those networks, or the networks themselves. A primary effect is to influence the adversary commander's decisions.

Network Defense Network defense (NetD) is employment of network-based capabilities to defend friendly information resident in or transiting through networks against adversary efforts to destroy, disrupt, corrupt, or usurp it. NetD can be viewed as planning, directing, and executing actions to prevent unauthorized activity in defense of Air Force information systems and networks and for planning, directing, and executing responses to recover from unauthorized activity should it occur.

Network Warfare Support Network warfare support (NS) is the collection and production of network related data for immediate decisions involving NW Ops. NS is critical to NetA and NetD actions to find, fix, track, and assess both adversaries and friendly sources of access and vulnerability for the purpose of immediate defense, threat prediction and recognition, targeting, access and technique development, planning, and execution in NW Ops.

4 – Electronic Warfare Operations

General Electronic warfare (EW) is any military action involving the use of electromagnetic or directed energy to manipulate the electromagnetic spectrum or to attack an adversary. The Air Force describes electronic warfare operations (EW Ops) as the integrated planning, employment, and assessment of military capabilities to achieve desired effects across the electromagnetic domain in support of operational objectives. The EW spectrum is not merely limited to radio frequencies but also includes optical and infrared regions as well. EW assists air and space forces to gain access and operate without prohibitive interference from adversary

systems and actively destroys, degrades, or denies opponents' capabilities, which would otherwise grant them operational benefits from the use of the electromagnetic spectrum.

Electronic Warfare Operations EW is a key contributor to air superiority, space superiority, and information superiority. The most important aspect of the relationship of EW to air, space, and information operations is that EW enhances and supports all operations throughout the full spectrum of conflict. Air Force EW resources and assets may take on new roles in support of operations as the electronic warfare operation mission evolves. The three military capabilities of EW operations are electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). All three contribute to air and space operations, including the integrated IO effort. Control of the electromagnetic spectrum is gained by protecting friendly systems and countering adversary systems.

Electronic attack (EA) is the division involving the use of electromagnetic, directed energy (DE), or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of deceiving, disrupting, denying, and/or destroying adversary combat capability. It also deceives and disrupts the enemy integrated air defense system (IADS) and communications, as well as enables the destruction of these adversary capabilities via lethal strike assets.

Electronic protection (EP) enhances the use of the electronic spectrum for friendly forces. Electronic protection is primarily the defensive aspect of EW that is focused on protecting personnel, facilities, and equipment from any effects of friendly or adversary employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability.

Electronic warfare support (ES), the collection of electromagnetic data for immediate tactical applications (e.g., threat avoidance, route selection, targeting, or homing), provides information required for timely decisions involving electronic warfare operations.

5 – Information Operations Planning and Execution

Information operations are integral to military operations and are a prerequisite for information superiority. IO supports, and may also be supported by, air, space, and cyberspace operations and needs to be planned and executed just like air operations. IO should be seamlessly integrated with the normal campaign planning and execution process. There may be campaign plans that rely primarily on the capabilities and effects an IO strategy can provide, but there should not be a separate IO campaign plan.

One of the commander's priorities is to achieve decision superiority over an adversary by gaining information superiority and controlling the information environment. This goal does not in any way diminish the commander's need to achieve air, space, and cyberspace superiority but rather facilitates efforts in those areas and vice versa. The aim of information superiority is to have greater situational awareness and control than the adversary. Effective use of IO leads to information superiority. The effort to achieve information superiority depends upon two fundamental components: an effects-based approach and well-integrated IO planning and execution accomplished by IO organizations.

Effects-Based Approach The ability to create the effects necessary to achieve campaign objectives, whether at the strategic, operational, or tactical levels, is fundamental to the success of the Air Force. An effect is the anticipated outcome or consequence that results from a particular military operation. The emphasis on effects is as crucial for successful IO as for any other airpower function. Commanders should clearly articulate the objectives or goals of a given military operation. Effects should then flow from objectives as a product of the military operations designed to help achieve those objectives. Based on clear objectives, planners should design specific operations to achieve a desired outcome and then identify the optimum capability for achieving that outcome. It is important to realize that operational assessment may

be more challenging in IO because the effects are often difficult to measure. IO may also be based upon common sense, a rule of thumb, simplification, or an educated guess that reduces or limits the search for solutions in domains that are difficult or poorly understood. For example, psychological effects are not only difficult to measure; they may also not manifest themselves until later in time. There are also second-order and third-order effects that should be taken into consideration, and again, these may not manifest themselves until much later. IO presents additional challenges in effects-based planning as there are many variables. Many of these variables also have human dimensions that are difficult to measure, may not be directly observable, and may also be difficult to acquire feedback. At all times, objectives must be set and effects must be analyzed from the point of view of the culture where operations are being conducted.

Information Operations Organizations A number of Air Force organizations contribute to effective IO. The following discuss several of the key organizations employed in information operations.

Information Warfare Flight (IWF) IO can be conducted throughout the spectrum of peace and conflict. In peacetime, the major command/numbered air force (MAJCOM/NAF) IWF is the operational planning element for IO and may coordinate IO actions when an air operations center (AOC) has not been activated. When the AOC is activated, a portion of the IWF is established as an IO team and integrates into the warfighting divisions within the AOC (Strategy, Plans, ISR, Combat Operations, etc.). The IO team provides the IO expertise to plan, employ, and assess IO capabilities prior to the initiation of hostilities, transition to conflict, and reconstitution.

EW Ops Organizations Electronic warfare is conducted by units with capabilities ranging across the electronic attack, protect, and support functions. EW operations require attention before, during, and after military operations. A joint EW coordination cell (EWCC) is the necessary planning and execution organization to orchestrate the activities of units to achieve EW objectives of the campaign plan.

Network Defense and Network Operations Organizations NetD and NetOps organizations provide the JFC with critical capabilities to realize the effects of information and decision superiority. Collectively, these organizations provide varying degrees of NetD and NetOps support. They provide commanders with real-time intrusion detection and perimeter defense capabilities, network management and fault resolution activities, data fusion, assessment, and decisions support. During employment, the organizations are arranged into a three-tiered operational hierarchy, which facilitates synchronized application of their collective capabilities in support of the DOD's defense-in-depth security strategy.

6 – Integrated Control Enablers

Information operations are dependent on integrated control enablers. The integrated control enablers are critical capabilities required to execute successful air, space, and information operations and produce integrated effects for the joint fight. These include intelligence, surveillance, and reconnaissance (ISR), network operations (NetOps), predictive battlespace awareness (PBA), and precision navigation and timing (PNT).

Network Operations and Information Assurance NetOps encompasses information assurance (IA), system and network management, and information dissemination management. The Air Force and joint community have come to recognize these pillars as information assurance and network defense, enterprise service management/network management, and content staging/information dissemination management respectively. NetOps consists of organizations, procedures, and functionalities required to plan, administer, and monitor Air

Force networks in support of operations and also to respond to threats, outages, and other operational impacts.

Information assurance comprises those measures taken to protect and defend information and information systems by ensuring their availability, integrity, authenticity, confidentiality, and non-repudiation (ability to prove sender's identity and prove delivery to recipient). IA spans the full lifecycle of information and information systems. IA depends on the continuous integration of trained personnel, operational and technical capabilities, and necessary policies and procedures to guarantee continuous and dependable information, while providing the means to efficiently reconstitute these vital services following disruptions of any kind, whether from an attack, natural disaster, equipment failure, or operator error. In an assured information environment, warfighters can leverage the power of the information age.

Intelligence, Surveillance, and Reconnaissance Global integrated ISR is cross-domain synchronization and integration of the planning and operation of ISR assets; sensors; processing, exploitation and dissemination systems; and analysis and production capabilities across the globe to enable current and future operations. ISR is a critical function that helps provide the commander the situational and battlespace awareness necessary to successfully plan and conduct operations. Commanders use the intelligence information derived from ISR assets to maximize their own forces' effectiveness by optimizing friendly force strengths, exploiting adversary weaknesses, and countering adversary strengths.

Predictive Battlespace Awareness Effective IO depends upon successful PBA. As a maturing concept, PBA is "the understanding of the operational environment that allows the commander and staff to correctly anticipate future conditions, assess changing conditions, establish priorities, and exploit emerging opportunities while mitigating the impact of unexpected adversary actions" (Air Force Pamphlet 14-118). PBA results from combining intelligence preparation of the operational environment (IPOE), ISR planning and synchronization, and ISR management into a coherent framework that maximizes the capabilities of ISR assets in all environments. IPOE is the analytical process used by intelligence organizations to produce intelligence estimates and other intelligence products in support of the commander's decision-making process. It is a continuous process that includes defining the operational environment; describing the impact of the operational environment; evaluating the adversary; and determining adversary courses of action.

Precision Navigation and Timing Precision navigation and timing provided by space-based systems enable IO by providing the ability to synchronize and guide IO force application to create effects across the battlespace.

Note: End of AFDD 3-13 extract.

Updated: September 2011

This Page Intentionally Blank

III. ORGANIZATIONS

This section includes a description of the following organizations:

- **Department of State**
- **National Agencies**
- **Department of Defense**
- **Joint Organizations and Educational Institutions**
- **Service Information Operations Organizations**

This Page Intentionally Blank

Department of State

Under Secretary of State for Public Diplomacy and Public Affairs

The Acting Under Secretary of State for Public Diplomacy and Public Affairs, Ann S. Stock, leads America's public diplomacy efforts, which seek to better understand, inform, and influence foreign publics. The Department of State's wide-ranging outreach activities include communications with international audiences, cultural programming, academic grants, educational and professional exchanges, and U.S. government efforts to confront ideological support for terrorism. These functions are indispensable to the conduct of foreign policy. Public diplomacy field operations are carried out by more than 1000 public diplomacy officers based in over 200 embassies, consulates, and other missions abroad. The Office of the Under Secretary has defined five strategic imperatives for 21st Century Public Diplomacy:

1. Shape the narrative
2. Better inform policy making
3. Expand and strengthen people-to-people relationships
4. Deploy resources in line with current U.S. government foreign policy priorities
5. Combat violent extremism

The Under Secretary directly supervises three bureaus (International Information Programs, Educational and Cultural Affairs, and Public Affairs). Within the Under Secretariat, the Office of Policy, Planning, and Resources focuses on the Department of State's long-range public diplomacy strategic policy, planning, and management of resources. A Center for Strategic Counterterrorism Communications was created in 2010 as an interagency collaboration to counter violent extremist propaganda. The Under Secretary also is the Administration's voting representative on the Broadcasting Board of Governors, the executive agency that directs American civilian international broadcasting (Voice of America, RFE/RL, Radio Marti, Radio Sawa, Al Hurra, and other radio and television programming aimed at foreign audiences).

1. Office of Policy, Planning and Resources for Public Diplomacy and Public Affairs (R/PPR): Reporting directly to the Under Secretary, R/PPR provides long-term strategic policy planning and coordination within the Department and with the interagency community for public diplomacy and public affairs programs. It also advises the Under Secretary on the allocation of resources appropriated by Congress for the conduct of public diplomacy and public affairs in order to focus those resources on the most urgent national security objectives.
2. Center for Strategic Counterterrorism Communications (R/CSCC): With support from DoD, the Intelligence Community, and other interagency partners, the State Department established the Center for Strategic Counterterrorism Communications (CSCC). The CSCC is housed within the Under Secretariat, reporting directly to Acting U/S Stock. It coordinates, orients, and informs U.S. government-wide communications regarding

terrorism and violent extremism with international audiences, to counter the al-Qaida narrative and radicalization of at-risk communities.

3. Bureau of Educational and Cultural Affairs (ECA): ECA fosters mutual understanding between the people of the United States and other countries. It does this in close cooperation with embassies and consulates abroad through academic, cultural and professional exchanges, as well as presenting U.S. history, society, art, and culture in all of its diversity to overseas audiences. The bureau manages the prestigious Fulbright Scholars program as well as the International Visitor Leadership Program. Many alumni of these programs have gone on to become heads of state, heads of government, government ministers, and leaders in their fields. Youth exchanges, English teaching programs, work-study exchanges, and university-to-university linkages are other programs that reach out to the next generation of leaders and promote mutual understanding and support for U.S. foreign policy. ECA awards millions of dollars in grants to American organizations for specific initiatives, while public diplomacy officers in the field have authority to grant funds to host nation institutions, NGO's, and individuals in support of strategic imperatives.
4. Bureau of International Information Programs (IIP): By providing international strategic communications for the foreign affairs community, IIP informs, engages, and influences international audiences about U.S. policy and society to advance America's interests. IIP programs move beyond policy dissemination and broadcasting to meaningful, sustained interaction with audiences around the world through social media, foreign language websites, publications, new technologies, and subject matter experts who are recruited to interact with foreign audiences through digital video conferences, in-country speaking engagements, lectures, and face-to-face discussions. The bureau runs six regional outreach offices to provide training in new media and packaged content for overseas posts. IIP also supports over 700 "American Spaces" around the world, ranging from the traditional American Center to its newest high-tech media platform. The bureau is prohibited from disseminating its products to the U.S. domestic audience by the Smith-Mundt Act and amendments.
5. Bureau of Public Affairs (PA): PA helps Americans understand U.S. foreign policy and the importance of foreign affairs by responding to press inquiries; holding press briefings; hosting "town meetings" and other conferences around the United States; arranging local, regional, and national newspaper, radio, television, and social media interviews with key Department officials; and providing audio-visual products and services. The bureau coordinates closely with press offices in the National Security Council, Department of Defense, and other agencies to ensure consistency in public affairs messages on foreign policy and conducts a daily press briefing for U.S. and international media accredited to the Department. Transcripts are posted daily. The bureau includes the office of the Department's spokesperson, who usually accompanies the Secretary of State on travel. The bureau also maintains the State Department public website at http://www.state.gov and a telephone information line (202-647-6575) for public inquiries. In addition, the Office of the Historian provides historical research and advice for the Department of State and publishes the official documentary history of U.S. foreign policy.

Website: http://www.state.gov/r/

Updated: October 2011

The Center for Strategic Counterterrorism Communications

The Center for Strategic Counterterrorism Communications (CSCC) was established in September 2010 to coordinate, orient, and inform government-wide public communications activities directed at audiences abroad and targeted against violent extremists and terrorist organizations, with particular focus on al-Qa'ida and associated movements. CSCC is based in the Department of State and operates under the broad policy direction of the White House, with interagency personnel and support. CSCC Coordinator Ambassador Richard LeBaron reports to the Under Secretary of State for Public Diplomacy and Public Affairs, and works closely with the Secretary of State's Coordinator for Counterterrorism (S/CT), other Department of State bureaus, and other government agencies.

Staffed by officers from multiple government agencies and the military, CSCC is comprised of two interactive components. The Integrated Analysis component leverages the Intelligence Community, academics, and other substantive experts to provide context and feedback for communicators. The Plans and Operations component leverages this input to devise effective ways to counter terrorist narratives and misinformation, in collaboration with U.S. embassies and consulates, interagency partners, and outside experts. CSCC's operations also include the work of the CSCC Digital Outreach Team (DOT), which challenges and counters extremist messages online in Arabic and Urdu, including through original video content. The DOT will add capacity in Somali in the near future.

In her speech in New York marking the 10th anniversary of 9/11, Secretary Clinton highlighted the mission of CSCC, noting that it "is tightly focused on undermining the terrorist propaganda and dissuading potential recruits. The center is housed at the State Department, but is a true whole-of-government endeavor. It has a mandate from the President. And as part of this effort, a group of tech savvy specialists – fluent in Urdu and Arabic – that we call the Digital Outreach Team are contesting online space, media websites and forums where extremists have long spread propaganda and recruited followers. With timely posts, often of independent news reports, this team is working to expose al-Qa'ida's and extremists' contradictions and abuses, including its continuing brutal attacks on Muslim civilians."

President Obama on September 9, 2011 signed Executive Order 13584, that assigns specific responsibilities and functions to the Center, in order to "reinforce, integrate, and complement public communications efforts across the executive branch that are (1) focused on countering the actions and ideology of al-Qa'ida, its affiliates and adherents, and other international terrorist organizations and violent extremists overseas, and (2) directed to audiences outside the United States. This collaborative work among executive departments and agencies brings together expertise, capabilities, and resources to realize efficiencies and better coordination of U.S. Government communications investments to combat terrorism and extremism."

In addition, the Executive Order established an interagency steering committee to provide advice to the Secretary of State on the operations and strategic orientation of CSCC and to ensure adequate support for it. The Executive Order also created a temporary support office as

a mechanism to facilitate the development of CSCC as it further implements whole-of-government public communications activities directed at audiences abroad, through personnel with relevant expertise detailed from other agencies, assistance, services, and other support.

Updated: October 2011

National Agencies

National Security Agency (NSA)

National Security Agency/Central Security Service (NSA/CSS)

Introduction

The National Security Agency / Central Security Service (NSA/CSS) is the home to America's codemakers and codebreakers, The National Security Agency has provided timely information to U.S. decision makers and military leaders for more than half a century. The Central Security Service was established in 1972 to promote a full partnership between NSA and the cryptologic elements of the armed forces.

NSA/CSS is unique among the U.S. defense agencies because of our government-wide responsibilities. NSA/CSS provides products and services to the Department of Defense, the Intelligence Community, government agencies, industry partners, and select allies and coalition partners. In addition, we deliver critical strategic and tactical information to war planners and war fighters.

Executive Order No. 12333, dated 4 December 1981, as recently amended (July 2008) describes the responsibilities of the NSA/CSS in more detail. The resources of the NSA/CSS are organized for the accomplishment of two national missions:

The Signals Intelligence (SIGINT) mission allows for an effective, unified organization and control of all foreign signals collection and processing activities of the U.S. The NSA/CSS is authorized to produce SIGINT in accordance with the objectives and priorities established by the Director of National Intelligence in consultation with the President's Foreign Intelligence Advisory Board. Foreign signals collection is a Title 50 United States Code (USC) authority given to the Director, NSA/CSS.

The Information Assurance (IA) mission provides the IA and Computer Network Defense (CND) solutions/services, and conducts Defensive Information Operations (DIO) in order to protect information processed by U.S. national security systems. The intent is to measurably improve the security of critical operations and information by providing know-how and technology to our suppliers, partners and clients, when and where they need them. The NSA/CSS's IA mission is authorized by National Security Directive 42.

The NSA/CSS is America's cryptologic organization. It produces foreign signals intelligence and performs highly specialized activities to protect U.S. Government national security information systems. A high technology organization, the NSA/CSS is on the frontiers of communications and data processing. It is also one of the most important centers of foreign language analysis and research within the U.S. Government. It is said to be the largest employer of mathematicians in the U.S. and perhaps the world. Its mathematicians design cipher systems

that search for weaknesses in adversaries' systems/codes and that protect the integrity of U.S. systems.

SIGINT is a unique discipline with a long and storied past. Its modern era dates to World War II, when the U.S. broke the Japanese military code and learned of plans to invade Midway Island. This intelligence allowed the U.S. to defeat Japan's superior fleet. The use of SIGINT is believed to have directly contributed to shortening the war by at least one year. Today, SIGINT continues to play an important role in keeping the United States a step ahead of its enemies.

The IA mission becomes increasingly more challenging as the world becomes more technology-oriented. IA professionals go to great lengths to make certain that Government systems remain impenetrable. The NSA/CSS supports the highest levels of the U.S. Government to the war fighter.

The NSA/CSS conducts one of the U.S. Government's leading Research and Development (R&D) programs. Some of the Agency's R&D projects have significantly advanced the state of the art in the scientific and business worlds. The NSA/CSS's early interest in cryptanalytic research led to the first large-scale computer and the first solid-state computer, predecessors to modern computing. The NSA/CSS also made ground-breaking developments in semiconductor technology and remains a world leader in many technological fields.

Technology and the world change rapidly, and great emphasis is placed on staying ahead of these changes with employee training programs. The National Cryptologic School is indicative of the Agency's commitment to professional development. The school not only provides unique training for the NSA workforce, but it also serves as a training resource for the entire Department of Defense (DoD). The NSA/CSS sponsors employees for bachelor and graduate studies at the Nation's top universities and colleges, and selected Agency employees attend the various war colleges of the U.S. Armed Forces.

Most NSA/CSS employees, both civilian and military, are headquartered at Fort Meade, Maryland, centrally located between Baltimore, MD and Washington, DC. Its workforce represents an unusual combination of specialties: analysts, engineers, physicists, mathematicians, linguists, computer scientists, researchers, as well as customer relations specialists, security officers, data flow experts, managers, administrative officers and clerical assistants.

SIGINT Mission

The NSA/CSS collects, processes and disseminates foreign SIGINT. The old adage that "knowledge is power" has perhaps never been truer than when applied to today's threats against our nation and the role SIGINT plays in overcoming them.

The NSA/CSS's SIGINT mission protects the nation by: Providing information in the form of SIGINT products and services that enable our government to make critical decisions and operate successfully; Protecting the rights of U.S. citizens by adhering to the provisions of the 4th amendment to the Constitution and; Using the nation's resources responsibly, according to the best management processes available.

Other Intelligence Community (IC) agencies are responsible for other types of intelligence: Central Intelligence Agency (CIA) - Human Intelligence (HUMINT); Defense Intelligence Agency – HUMINT and Measurement and Signature Intelligence (MASINT) and; National Geospatial Agency (NGA) – Imagery Intelligence.

These different yet complementary disciplines give our nation's leaders a greater understanding of the intentions of our adversaries.

The NSA/CSS's SIGINT mission provides our military leaders and policy makers with intelligence to ensure our national defense and to advance U.S. global interests. This information is specifically limited to that on foreign powers, organizations or persons and international terrorists. The NSA/CSS responds to requirements levied by intelligence customers, which includes all departments and levels of the U.S. Executive Branch of Government.

The prosecution of the SIGINT mission has evolved from the relatively static, industrial age, Cold War communications environment to the ubiquitous, high speed, multi-functional technologies of today's information age. The ever-increasing volume, velocity and variety of today's communications make the production of relevant and timely intelligence for military commanders and national policy makers more challenging than ever.

As much as modern telecommunications technology poses significant challenges to SIGINT, the many languages used in the nations and regions of the world that are of interest to our military and national leaders require the NSA/CSS to maintain a wide variety of language capabilities. Successful SIGINT depends on the skills of not only language professionals but those of mathematicians, analysts, and engineers as well. The nation is indebted to them for the successes they have won.

IA Mission

IA is one of the two core missions of the NSA/CSS. The Information Assurance Directorate (IAD) is dedicated to providing IA solutions that will keep U.S. national security systems safe from harm.

IA refers to the measures intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

The IAD's mission involves detecting, reporting, and responding to cyber threats; making encryption codes to securely pass information between systems; and embedding IA measures directly into the emerging DoD's Global Information Grid (GIG). It includes building secure audio and video communications equipment, making tamper protection products, and providing trusted microelectronics solutions. It entails testing the security of customers' systems, providing Operations Security (OPSEC) assistance, and evaluating commercial software and hardware against nationally set standards to better meet our nation's needs.

The IAD's mission has evolved through three very distinct stages: Communications Security (COMSEC), Information Systems Security (INFOSEC), and IA. Following World War II and the Korean War, efforts focused primarily on cryptography (i.e. designing and building encryption devices to provide confidentiality for information). COMSEC is defined as the measures taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptographic security, transmission security, emission security, and physical security of COMSEC material.

In the 1980s, the introduction and widespread use of computers created new demands to protect information exchanges between interconnected computer systems. This demand created the Computer Security (COMPUSEC) discipline. However, the community recognized that stand-alone COMSEC and COMPUSEC activities could not protect information during storage, processing or transfer between systems. This recognition gave rise to the term INFOSEC and the information protection mission took on a broader perspective. INFOSEC is defined as the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to

authorized users, including those measures necessary to detect, document, and counter such threats.

In the 1990s, IA emerged and focused on the need to protect information during transit, processing, or storage within complex and/or widely dispersed computers and communication system networks. IA also includes a dynamic dimension where the network architecture is itself a changing environment, including the information protection mechanisms and features that detect attacks and enable a response to those attacks. IA measures protect against the exploitation or penetration efforts routinely conducted by sophisticated adversaries, but also protect against hackers or criminals from creating havoc across layered domains.

Today, IA incorporates more than just the need for confidentiality achieved through the use of encryption products that the NSA/CSS produces or certifies. IA also includes the DIO elements that protect and defend information and information systems.

The Director of the National Security Agency/Central Security Service, a four-star military position, is dual-hatted as the Commander, U.S. Cyber Command.

Contact Information: NSA Visiting Professor, U.S. Army War College (717) 245-4727

Website: http://www.nsa.gov/

Updated: October 2011

Department of Defense

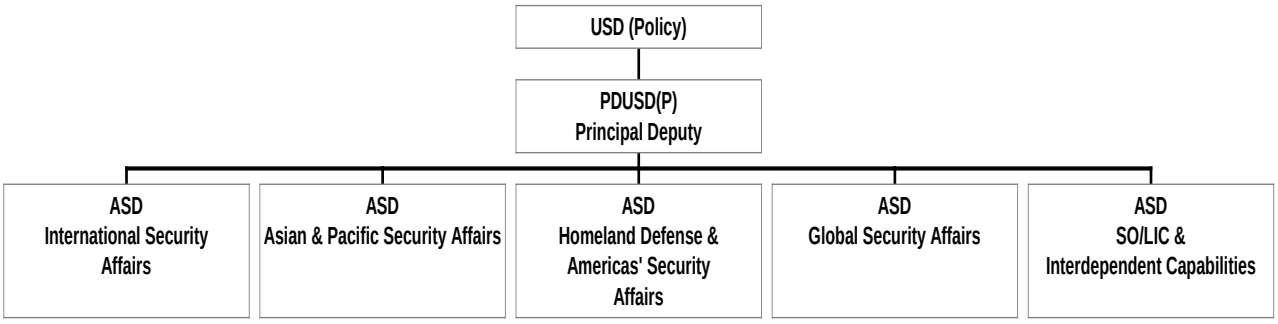
This section includes a description of the following organizations:

- **Under Secretary of Defense – Policy (USD(P))**
- **Assistant Secretary of Defense for Public Affairs, Communication Planning and Integration (CPI)**
- **Department of Defense Chief Information Officer (DoD CIO)**
- **Defense Information Systems Agency (DISA)**
- **Information Assurance Technology Analysis Center (IATAC)**

This Page Intentionally Blank

Under Secretary of Defense – Policy (USD(P))

Mission: The mission of the Office of the Under Secretary of Defense for Policy is to consistently provide responsive, forward-thinking, and insightful policy advice and support to the Secretary of Defense, and the Department of Defense, in alignment with national security objectives.



The responsibilities of the USD(P) include but are not limited to the following:

- Represent the Department of Defense, as directed, in matters involving the National Security Council (NSC); the Department of State; and the other Federal Departments, Agencies, and inter-Agency groups with responsibility for national security policy.
- Serve as a member of the NSC Deputies Committee; serve as a member of the Deputies Committee for Crisis Management; and advise the Secretary of Defense on crisis prevention and management, including contingency planning for major areas of concern.
- Develop DoD policy guidance, provide overall supervision, and provide oversight of planning, programming, budgeting, and execution of special operations activities, including civil affairs and psychological operations, and of low-intensity conflict activities, including counter-terrorism, support to insurgency, and contingency operations.
- Develop policy and provide oversight for emergency planning and preparedness, crisis management, defense mobilization in emergency situations, military support to civil authorities, civil defense, and continuity of operations and government. Develop policy and coordinate DoD participation in, and exercise staff supervision over, special activities, special access programs, sensitive support to non-DoD agencies, and the joint worldwide reconnaissance schedule.

The roles and responsibilities of the Principal Deputy and the five Assistant Secretaries are described below:

Principal Deputy Undersecretary of Defense for Policy – Provides advice and assistance to the Secretary of Defense, Deputy Secretary of Defense and the Under Secretary of Defense for Policy on national security policy, military strategy, and defense policy.

The Assistant Secretary of Defense for International Security Affairs – Serves as the principal advisor to the USD(P) and the Secretary of Defense on international security strategy and policy on issues of DoD interest that relate to the nations and international organizations of Europe (including the North Atlantic Treaty Organization), the Middle East, and Africa, their governments and defense establishments; and for oversight of security cooperation programs and foreign military sales programs in these regions.

The Assistant Secretary of Defense for Asian and Pacific Security Affairs – Serves as the responsible official for U.S. security and defense policy in the Asia-Pacific region.

The Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs – Oversees the operations of the following offices:

- Office of the Deputy Assistant Secretary of Defense for Homeland Defense & Defense Support to Civil Authorities (DSCA)
- Office of the Deputy Assistant Secretary of Defense for Western Hemisphere Affairs
- Office of Deputy Assistant Secretary of Defense for Crisis Management and Mission Assurance

The responsibilities of the ASD for Homeland Defense and Americas Security Affairs and these three offices can be found at http://policy.defense.gov/hdasa/index.aspx.

The Assistant Secretary of Defense for Global Strategic Affairs – Oversees the operations of the following offices:

- Office of the Deputy Assistant Secretary of Defense for Countering Weapons of Mass Destruction (WMD)
- Office of the Deputy Assistant Secretary of Defense for Nuclear and Missile Defense Policy
- Office of the Deputy Assistant Secretary of Defense for Cyber Policy
- Office of the Deputy Assistant Secretary of Defense for Space Policy

The Assistant Secretary of Defense for Special Operations/Low Intensity Conflict – Serves as the principal civilian advisor to the USD(P) and the Secretary of Defense on special operations and low-intensity conflict matters. The ASD(SO/LIC)'s principal duty is the overall supervision (to include oversight of policy and resources) of special operations and low-intensity conflict activities. These core tasks, according to USSOCOM's 2007 Posture Statement, include counterterrorism, unconventional warfare, direct action, special reconnaissance, foreign internal defense, civil affairs, information and psychological operations, and counter-proliferation of WMD.

In addition to policy oversight for special operations and stability operations capabilities, ASD(SO/LIC) has policy oversight for strategic capabilities, and force transformation and resources. This includes oversight of capability development to include general-purpose forces, space and information capabilities, nuclear and conventional strike capabilities, and missile defense. As such, ASD(SO/LIC), after the Secretary and Deputy Secretary, will be the principal official charged with oversight over all warfighting capabilities within the senior management of the Department of Defense.

The following offices fall under the ASD for Special Operations/Low Intensity Conflict and Interdependent Capabilities:

- Office of the Deputy Assistant Secretary of Defense for Special Operations and Combating Terrorism (DASD(SOCT))
- Office of the Deputy Assistant Secretary of Defense for Counternarcotics and Global Threats
- Office of the Deputy Assistant Secretary of Defense for Partnership Strategy and Stability Operations

Based on a front-end assessment ordered by the Secretary of Defense, USD(P) assumed the functions of the Principal Staff Advisor (PSA) to the Secretary for information operations (IO) in early 2011. In addition, USD(P) undertook an expanded role in DoD's strategic communications

(SC) policy. As a result of this realignment and expansion, the following actions have taken place:

- The personnel and resources that support DoD IO activities have moved from the Under Secretary of Defense for Intelligence (USD(I)) to the USD(P). This resulted in the establishment of a new IO Directorate under the DASD(SOCT), who reports to the ASD(SOLIC). Through the Senior Director of the IO Directorate, the USD(P) will exercise oversight of all DoD IO activities. USD(I) continues to support IO as the SecDef's PSA for intelligence, counterintelligence, and security.
- The USD(P) now co-chairs the Global Engagement Strategic Communications Committee (GESCC) with the ASD for Public Affairs. The GESCC is the Department's SC coordination body that reviews DoD activities for consistency with national directives and represents DoD on Interagency SC matters.

Website: http://policy.defense.gov/

Updated: October 2011

This Page Intentionally Blank

Assistant Secretary of Defense for Public Affairs – Communication Planning and Integration (CPI)

Background/Overview. The rapid pace of evolution in the global information environment requires the Department of Defense (DoD), in conjunction with other U.S. Government (USG) departments and agencies, to develop and constantly improve strategic communication (SC) processes, particularly by exploring innovative approaches and cross-agency integration of best practices and "what works."

At its most basic, SC is the orchestration of actions, images, and words to achieve desired effects. SC is the process of coordinating horizontally (across DoD and the USG, as well as with international partners when appropriate) and vertically (up and down the chain of command) to:

- Close the "say-do gap";
- Consider information and communication as part of strategy, planning and policy development from the very beginning;
- Assess communication impacts of actions before taking actions;
- Consider "soft power" capabilities equally with more traditional DoD kinetic capabilities when determining the optimum course of action; and
- Integrate issues of audience and stakeholder perception into policy-making, planning, and operations at every level.

SC planning goes beyond a single operation or bilateral engagement, focusing on the region, operating environment and globe. It's also less about "sending a message" and more about engagement. More than ever, efforts to listen to and understand different perspectives and cultures must be deliberately planned and integrated into the decision cycle of all diplomats and joint force commanders to ensure America's future success.

Doctrine. SC comprises the focused processes and efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable to advance national interests and strategic objectives by coordinating actions and information, synchronized with other elements of national power. (Revised definition submitted for inclusion in JP 5-0 update.)

SC is a natural extension of strategic direction and supports the President's strategic guidance, the National Defense Strategy, and the National Military Strategy. SC planning establishes unity of US themes and messages, emphasizes success, accurately confirms or refutes external reporting on US operations, and reinforces the legitimacy of US goals. This is an interagency effort, which provides an opportunity to advance US regional and global partnerships. (JP 5-0)

The USG uses SC processes to provide top-down guidance relative to using the informational instrument of national power in specific situations, but SC is addressed throughout the planning process at all levels – from strategic to tactical – to align regional or functional end states with broader policy goals. SC is an enabling function that guides and informs actions, within organic processes, e.g., Joint Operational Planning, imbedded within existing structures.

Within the Pentagon, the primary functions involved in the SC synchronization process include: Strategy and Plans, Policy, Information Operations (IO), Military Information Support Operations (MISO), Defense Support to Public Diplomacy (DSPD), Military Diplomacy (MD), Public Affairs (PA), Civil Affairs (CA), Legislative Affairs, and Operations (with many supporting components) – all working together to accomplish military objectives that support national objectives.

Public diplomacy is the purview of the Department of State (DoS), but DoD provides direct support through DSPD and MD, and most DoD's efforts and activities overseas have direct diplomatic and public diplomacy impacts. Both Pentagon and combatant command (COCOM)

staffs coordinate continually with DoS and U.S. embassies around the world to ensure that DoD and DoS efforts are integrated, mutually supportive, and achieve national objectives.

DSPD and MD encompass a wide variety of activities and engagement programs that influence opinions and perceptions of foreign publics and militaries. Some examples of DSPD include Military Information Support Teams (MISTs) that provide direct support to US embassies and news and informational websites in target audience native languages in several theaters. Additionally, planned humanitarian assistance programs, as well as disaster relief operations, have public diplomacy impacts. Examples of MD include formal bilateral programs between DoD and the Ministry of Defense of another nation, DoD civilian and military senior leader engagement with their counterparts in other nations, and "mil-to-mil" engagement and joint training programs between U.S. units and foreign military units.

Note: DoS does not use "SC" as an overarching concept but rather recognizes SC as parallel, and sometimes synonymous, to Public Diplomacy (PD). The Under Secretaries of State for Public Diplomacy and Public Affairs have generally used "Public Diplomacy and Strategic Communication" or "SC and PD."

Mission. CPI, formerly known as DASD(JC) was created in December 2005 to assist the Assistant Secretary of Defense (Public Affairs) (ASD(PA)) in shaping DoD-wide processes, policy, doctrine, organization, and training of the primary communication supporting capabilities, particularly public affairs and visual information. CPI has assumed many of the strategic communication planning responsibilities and functions previously performed by the Strategic Communication Integration Group (SCIG) Secretariat, disbanded in early 2008.

CPI leads communication planning and integration on strategic issues and mid- to long-range efforts, to ensure that communication plans and strategies are coordinated and synchronized across the Department and with other USG agencies, and that ASD(PA) equities are represented to maximize DoD's capability to communicate in an aggressive and synchronized manner.

Communication planning and integration activities focus on issues, trends, and objectives of broad scope and importance to the Office of the Secretary of Defense (OSD), the Chairman of the Joint Chiefs of Staff (CJCS), the COCOMs, the Military Services, and other government departments. CPI facilitates vertical and horizontal coordination, integration, and synchronization of planning efforts across DoD and among USG departments. It also focuses on how best to inform, educate and persuade key audiences on significant issues. Finally, it aims to capture, aggregate and share knowledge developed by COCOMs and others.

CPI is the principal advisor to the ASD(PA) on and representative to the Building Partnership Capability Portfolio Management (BP CPM) process, especially Joint Capability Area (JCA) Tier 2: Communicate, and communication-related issues in the Quadrennial Defense Review (QDR).

Composition. CPI consists of a group of strategic planners, each with responsibility for support to a number of COCOMs and/or Services; the office works in direct coordination with Office of the Under Secretary of Defense for Policy (OUSD(P), and with the Joint Staff (primarily the office of the Deputy Director for Information and Cyberspace Policy, under the Director, Strategic Plans and Policy (J-5 DDICP)). Representatives from these offices, plus the Office of the Under Secretary of Defense for Intelligence (OUSD(I)) and others, regularly convene as a Global Engagement Strategy Coordinating Committee (GESCC) at the DoD level, and key members also participate in the SC Interagency Policy Committee (IPC) at the NSC level.

Reporting Responsibilities. CPI supports the OUSD(P) in operational and interagency matters and represents and reports to the ASD(PA).

Updated: October 2011

Department of Defense Chief Information Officer (DoD CIO)

Overview: The DoD CIO is the principal staff assistant and advisor to the Secretary of Defense and Deputy Secretary of Defense on information technology, which includes national security systems (NSS); information resources management (IRM); command and control (C2); communications; radio frequency spectrum; information systems; information assurance (IA); cyber security; and positioning, navigation and timing (PNT).

Vision: To deliver agile and secure information capabilities to enhance combat power and decision making.

Mission: Information is one of our Nation's greatest sources of power. The first and greatest goal of the DoD CIO is to deliver that power to enable the achievement of mission success in all operations of the Department: warfighting, business, and intelligence.

Responsibilities and Functions:
The DoD CIO will:

a. Develop DoD strategy and policy on the operation and defense of all DoD IT and information systems
b. Serve as the Agency Chief Information Officer for the Department of Defense with the responsibilities, duties and qualification pursuant to section 11315 of title 40, United States Code (U.S.C.) (Reference (c)) and the additional responsibilities pursuant to section 2223 of title 10, U.S.C. (Reference (d))
c. Serve as the Chief Information Officer for the Department of Defense with the responsibilities pursuant to section 3506 of title 44, U.S.C. (Reference (e)) related to Federal Information Policy
d. Serve as DoD lead for DoD defensive cyber security operations
e. Lead and oversee strategic human capital planning for the DoD IT and information assurance (defensive cyber security) workforce
f. Serve as DoD lead for DoD communications and information networks
g. Direct, manage and provide policy guidance and oversight for the C2 and communications needs of the President and national security leadership
h. Serve as DoD lead for DoD spectrum management
i. Serve as DoD lead for positioning, navigation and timing (PNT) requirements
j. Serve as DoD lead for Command and Control (C2)
k. Lead core IT infrastructure and enterprise-wide IT initiatives

Headquarters: The headquarters for the DoD CIO organization is in the Pentagon, with staff elements both in the Pentagon and in nearby office buildings in Arlington, VA.

Website: http://cio-nii.defense.gov/

Updated: October 2011

This Page Intentionally Blank

Defense Information Systems Agency (DISA)

Mission: DISA, a Combat Support Agency, engineers and provides command and control capabilities and enterprise infrastructure to continuously operate and assure a global net-centric enterprise in direct support to joint warfighters, National level leaders, and other mission and coalition partners across the full spectrum of operations.

Vision: Leaders enabling information dominance in defense of our Nation.

DISA – An Operational Focus:
DISA is a Combat Support Agency with an operational focus providing joint and combined warfighting information technology capabilities. The agency's priority is to operate a core information infrastructure of networks, computing centers, and enterprise services (Internet-like information services) that connect 4,300 locations reaching 90 nations supporting Department of Defense and national interests. Engineering, acquisition, testing, and contracting functions support the incremental and modular improvements to this infrastructure, as well as day-to-day maintenance and sustainment requirements. Responsive and effective delivery of information solutions/capabilities is dependent upon on a cohesive lifecycle management process – a single execution arm accountable for all aspects of design, engineering, acquisition, implementation, sustainment and operation. This tightly coupled integration results in improved interoperability, reliability, availability, expandability, and recoverability of the enterprise infrastructure reducing costs at the same time as capability and capacity are increased. Currently, DISA is that execution arm synchronizing this continuous lifecycle and feedback process to deliver mission critical capabilities to the Department of Defense.

Agency Core Missions:

- Global Communications Services – Terrestrial/Satellite transport and voice/video/data
- Enterprise Computing Services – Hosting Joint Applications/Enterprise Services
- Defense Enterprise Services – Internet-like information services (e.g. discovery and collaboration)
- Mission Assurance Services – Protection of Infrastructure/Information
- Command and Control/Information Sharing – Situational awareness/decision making

Agency Special Missions:

- Enterprise Wide Systems Engineering – Making the GIG work end to end
- White House Communications – Information support to the President
- Joint Testing – Interoperability and operational testing
- Defense Spectrum – National and Department of Defense Solutions
- Joint Staff Support Center – Information support to National Military Command Center (NMCC) and Joint Staff leadership
- Defense IT Contracting – IT contracting and procurement services

- National/Senior Leadership and Nuclear Command, Control and Communications – Wired and wireless transport with voice, video, and services

Overview of DISA's 2011-12 Campaign Plan: http://www.disa.mil/About/Our-Campaign-Plan

Organizational structure: http://www.disa.mil/about/organization/index.html

Website: http://www.disa.mil/

Updated: September 2011

Information Assurance Technology Analysis Center (IATAC)

http://iac.dtic.mil/iatac/

IATAC is an Information Assurance (IA) Center of Excellence that is your one-stop shop for **free products and services**. We offer a free four-hour Technical Inquiry (TI) research service, free research materials, and other products and services. IATAC is also a contract vehicle that allows all Department of Defense (DoD) and federal agency customers to sponsor organization-specific, critical IA Research and Development (R&D) efforts. In its history, IATAC has performed IA and cybersecurity R&D on over 400 DoD and federal contracts. The resulting scientific and technical information from these contracts is shared and reused among the Defense Technical Information Center (DTIC) customers through DTIC Online Access Control (DOAC) - http://www.dtic.mil/dtic/announcements/DOAC.html, where DTIC customers can perform their own independent research.

Mission:
The Information Assurance Technology Analysis Center (IATAC) is one of ten Department of Defense Information Analysis Centers (IACs) sponsored by DTIC - http://www.dtic.mil/dtic/, a field operating agency under the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)) - http://www.acq.osd.mil/chieftechnologist/index.html. The other IACs provide similar products and services in their functional areas.

IATAC's mission is to provide DoD a central point of access for IA and cybersecurity to include emerging technologies in system vulnerabilities, R&D, models, and analysis to support the development and implementation of effective defense against information warfare attacks.

Free Products and Services:
All of the following products and more are available for free from the IATAC web site via a simple product request form, an email (iatac@dtic.mil), telephone call (703-984-0775), or via subscription:

- A free four-hour Technical Inquiry research service to answer authorized users' most pressing IA/cybersecurity questions. To answer these and other critical IA/cybersecurity questions, IATAC relies on its extensive Subject Matter Expert (SME) network, which includes retired senior military leaders, leading academic researchers, and industry executives who have contributed significantly to the advancement of IA and cybersecurity. Our SME's can help find answers to your particularly difficult questions. Past inquiries have included: have there been any interesting developments in balancing information sharing with information security requirements; what is Google Voice, how is it used, and why is or why is it not better than other similar products; what database security tools are currently used across the federal government; and are there any government or defense organizations that use Ruby on Rails?
- Free State of the Art Reports (SOARs) on the following IA topics: Security Risk Management for the Off-the-Shelf Information and Communications Technology Supply Chain, Measuring Cybersecurity and Information Assurance (IA), Insider Threat, and Software Security Assurance.
- Also available is a tools report database that contains information on a wide range of intrusion detection, vulnerability analysis, firewall applications, and anti-malware tools;

- A quarterly newsletter (*IAnewsletter)* that provides timely IA and cybersecurity articles; and
- An IA and cybersecurity "early-bird" called the *IADigest*.

What is an Authorized User?
Any DoD or federal government employee with a .mil or .gov email address and industry, academia, or contractor staff that register with DTIC.

Where is all this information? Register for DOAC:
Additional IA and cybersecurity information (and information from the other nine DoD IACs) that is available through DTIC via registration includes: millions of scientific and technical documents across a wide spectrum of topics from DOAC - http://www.dtic.mil/dtic/announcements/DOAC.html, as well as standard wiki collaboration and information from DoD Techipedia - https://www.dodtechipedia.mil/dodwiki. ***Registration is extremely easy for users possessing a Common Access Card (CAC).***

Management and Direction of IATAC Operations:
IATAC operates under the direction of DTIC with technical assistance provided by a government Executive Steering Committee. The committee is made up of 17 Senior IA and cybersecurity professionals from government, academia, and the DoD R&D community. They include representation from the Department of Homeland Security (DHS), Office of the Secretary of Defense's Defense Information Assurance Program (DIAP), U.S. Strategic Command (USSTRATCOM), U.S. Cyber Command (USCYBERCOM) , National Security Agency (NSA), Naval Postgraduate School (NPS), and other OSD offices to name a few. The Executive Steering Committee meets once a year and provides recommendations to the IATAC Contracting Officer Representative (COR) and the DoD IAC Program Management Office (PMO) regarding IATAC's operations, particularly the information management, collection, analysis, and dissemination efforts. Additionally, the Executive Steering Committee analyzes which IA topics are of greatest interest to the IA community and makes recommendations on topics for SOARs and technical reports that IATAC researches and produces based on these analyses.

Background:
On 14 July 2011, the Honorable William J. Lynn, III, Deputy Secretary of Defense, gave a speech at the National Defense University outlining the DoD Strategy for Operating in Cyberspace. He stated, "Because cyberspace is composed of many interwoven networks that perform many different functions, ensuring its peaceful use will require efforts on many fronts. The men and women of the military, other government agencies, our allies, the private sector, and indeed, the citizens of cyberspace must all play a role." Since its inception, IATAC has facilitated the sharing of IA and cybersecurity information across these groups in an effort to advance cyberspace protection. The United States is vulnerable to information events (and even information warfare activities), and this is exacerbated by the prolific use of information systems and computing networks across all four elements of power—economic, diplomatic/political, military, and informational. As a result, IA and cybersecurity professionals must be cognizant of the tenants of IA and cybersecurity—confidentiality, integrity, availability, authentication, and non-repudiation. Recent advances in information technology have made information systems easier to use, less expensive, and more available. Often ease of use comes at the expense of security, so we must be proactive in our security approach. Technologies such as cloud computing and mobile communications coupled with the unknowns in the supply chain related to the products, services, and components of all hardware and software only compound the already overly complex environment. Throw in the diverse nature of all federal government/DoD organizations, state and local organizations, and the many

industry and academic partners interfacing with all of these, and the situation demands a central information resource. IATAC is that resource.

The protection of DoD information systems and the automated systems that further our national objectives are of supreme importance to our national interest. IATAC provides a central repository for a wide range of IA and cybersecurity data, methodologies, models, and analyses of emerging technologies relating to the five tenants of IA and cybersecurity—confidentiality, integrity, availability, authentication, and non-repudiation. Our focus is R&D for the warfighter and we work closely with the PEO/PM and acquisition communities as well as others. IATAC's analysis extends across policy, doctrine, and strategy development, to R&D, science and technology, engineering, and architecture, as well as operations and training. This spectrum of activities ensures that management, collection, analysis, and dissemination of a broad and growing library of scientific and technical information (STI) related to IA and cybersecurity and the reuse of available STI to authorized users will continue. IATAC serves to help synchronize the IA and cybersecurity communities' efforts across the full spectrum of IA activities.

Location and Contact Information:
IATAC
13200 Woodland Park Road
Herndon, VA 20171
Phone: (703) 984.0775
FAX: (703) 984.0773
E-mail: iatac@dtic.mil
Website: iac.dtic.mil/iatac/

Updated: October 2011

This Page Intentionally Blank

Joint Organizations and Educational Institutions

The section includes a description of the following organizations:

- **Joint Staff, Deputy Director for Global Operations (DDGO)**
- **Joint Spectrum Center (JSC)**
- **Joint Public Affairs Support Element (JPASE)**
- **Joint Information Operations Warfare Center (JIOWC)**
- **U.S. Strategic Command (USSTRATCOM)**
    - **U.S. Cyber Command (USCYBERCOM)**
- **U.S. Special Operations Command (USSOCOM)**
- **Joint Forces Staff College – Information Operations Program**
- **Information Operations Center for Excellence Naval Postgraduate School**

This Page Intentionally Blank

Joint Staff, Deputy Director for Global Operations (DDGO J39)

Mission:
The Deputy Director for Global Operations (DDGO J-39) is responsible to the Director for Operations (DJ-3) and the Chairman of the Joint Chiefs of Staff (CJCS) for providing expertise and advice in coordinating joint global operations to include information operations (IO). The DDGO is responsible for IO activities, developing joint IO policy and doctrine, and coordinating with the Office of the Secretary of Defense (SecDef), combatant commands, Services, Defense Agencies, other staff directorates, the Intelligence Community, and interagency on IO issues/actions. In addition, the DDGO is the focal point for all Special Technical Operations (STO).

As of 1 October 2011, The Joint Information Operations Warfare Center (JIOWC) became a Chairman-controlled activity (CCA) under the supervision of the DJ-3. CCAs are specialized organizations designed to address unique areas that are of joint interest. The JIOWC supports the Joint Staff and combatant commands in DOD efforts to integrate joint information-related capabilities. The Director, JIOWC reports to the DJ-3 via the J-39.

Organization:
The DDGO contains five IO focused divisions:

The **Computer Network Operations Division (CNOD)** advises the SecDef and CJCS, through the DJ-3, on Computer Network Operations. Additionally, CNOD provides analyses and recommendations for the integration and synchronization of global cyberspace operations, including defense, exploitation and attack; network operations (NETOps); and information assurance/cyber security. CNOD also supports Combatant Commands (COCOMS) to meet Combatant Commander requirements and interfaces with the U.S. Government Interagency on operational employment and deconfliction of military CNO. Specific CNOD activities include:

- Provides operational expertise and operational assessments for Joint Staff issues relating to CNO
- Represent Joint Staff on the Department of Homeland Security National Cyber Response Coordination Group and other interagency efforts
- Planning and integration of CNO to support COCOMs through the Joint Operational Planning and Execution System (JOPES)
- Representing the Joint Staff at DoD and Interagency working groups, as necessary
- Providing On-call support to the National Joint Operations and Intelligence Center and NMCC for Cyberspace issues
- Providing input and oversight to exercises on the CJCS Exercise List and other major DoD and Interagency exercises with significant CNO activities

The **Information Operations Division (IOD)** facilitates and coordinates special capabilities and electronic warfare (EW) for the Chairman, in support of all COCOMs, SecDef and select interagency partners. Additionally, IOD educates operators to better plan and employ military Information Operations. Some of the tasks performed by IOD are:

- Support to COCOM requirements in EW and STO
- Coordinate, integrate and support COCOM efforts with SecDef and USG policies, plans and actions
- Advocate IO related COCOM issues to the interagency
- Serves as Joint Staff Advocate for Subject Matter Expert (SME) for Social Science Modeling
- Serve as Joint Staff SME for Counter Threat Finance
- Develop and coordinate Joint IO policy & doctrine
- Coordination w/OSD on IO issues and directives
- IO career force oversight
- Coordinates joint Operational Security (OPSEC) requirements; Provide OPSEC support to joint force commanders

IOD consists of the following branches: Combatant Command Support, Plans Support, Electronic Warfare, Intelligence Community Liaisons, Strategic Multi-layer Analysis Management, IO Policy and Doctrine.

The Military Information Support Division (MISO) provides expertise and advice on MISO employment to achieve national, strategic, and theater military objectives. It develops and provides guidance to, and coordinates with, COCOMs and Services; reviews COCOM OPLAN requirements; develops concepts and prepares MISO plans; develops and coordinates Joint MISO doctrine; publishes Joint MISO doctrine; and publishes MISO Supplements to the Joint Strategic Capabilities Plan and staff deployment orders. Some of the tasks performed by MISO are:

- Prepare, staff and transmit MISO specific execute orders, deployment orders, and MISO program approval
- Provide MISO SME to CJCS & Joint Staff, DoD, and United States Government (USG) Strategic Communication
- Assist in the development of joint MISO doctrine
- Serve as National Representative to NATO PSYOP working group

MISO consists of the following branches: Geographic Combatant Command Support and Program and Doctrine

The Special Actions Division (SAD) has primary responsibility for MILDEC and will work directly with JIOWC/Mission Support Division and with the Defense MILDEC Program Office as primary stakeholders to ensure community wide equities are maintained and synchronized. The SAD performs the following tasks:

- Develop and coordinate MILDEC joint doctrine publications
- Serve as the Joint Staff focal point office for the Defense Sensitive Support Program
- Coordinate all Defense Sensitive Support requirements between OSD and other Government agencies with the Services and Combatant Commanders

SAD is composed of the Support Activities Branch and the Tactical Security Branch.

The Joint Information Operations Center assists the Joint Staff in improving DoD ability to meet COCOM information-related requirements, improves development of information related capabilities, and ensures operational integration and coherence across COCOMs and other DoD activities.

- Provide combatant commands with the assessment tools and processes needed to evaluate the performance and effectiveness of IO
- Provide operational support to the Joint Staff, military services, and DoD agencies to assist in coordinating and integrating DoD IO operational support for joint commanders
- Facilitate sharing of IO best practices across the joint force
- Assist in the development of a joint IO force development strategy
- Support IO Integration and Assessment functions with tailored IO intelligence
- Support mission activities conducted within special access programs and under alternative compensatory control measures as direct by the Joint Staff

The Reconnaissance Operation Division is also in the Information Operations Division with a mission to recommend policy, establish procedures, and coordinate Secretary of Defense and Presidential approval for Sensitive Reconnaissance Operations worldwide. RDO is not an IO focused organization within DDGO.

Location:

The DDGO is located in the Pentagon.

Website: http://www.jcs.mil/

Updated: October 2011

This Page Intentionally Blank

Joint Spectrum Center (JSC)

Challenge: Military spectrum is a finite resource. The high tempo of global military operations and subsequent logistical support strain the already overcrowded spectrum bands.

Satellite communications and Intelligence, Surveillance, and Reconnaissance (ISR) platforms, including Unmanned Aerial Systems, consume large amounts of available spectrum. The increased need for added capacity in voice, data, and video communications create a demand for deliberate and synchronized spectrum operations across the Department of Defense. The Joint Spectrum Center is at the forefront of spectrum operations and supports the warfighter by providing complete, one-stop spectrum-related services to the military departments and combatant commands.

Mission: To enable effective and efficient use of the electromagnetic spectrum and control of electromagnetic effects in support of national security and military objectives.

Major Responsibilities

- Provide operational support in spectrum matters to the Joint Staff and Combatant Commands for contingencies, operations, exercises, and otherwise as requested.
- Conducts research and development into spectrum efficient technologies to improve the Department's use of spectrum.
- Facilitates global spectrum information exchange by developing protocols, standards, applications, information systems, and by influencing national and international spectrum regulations.
- Develops, maintains, and distributes spectrum engineering and Electromagnetic Environmental Effects (E3) analysis models, simulations, software, and data.
- Develops, distributes, and conducts E3 and spectrum management training courses for DoD Components.
- Provides technical E3 and spectrum engineering support to minimize interference, collateral impacts, detection, or operational restrictions for DoD components.

JSC Functional Components

J3 Operations Division – Provides remote and/or deployed spectrum management training and support to the Joint Staff, Combatant Commands, joint force commanders, and intelligence community. Spectrum management support consists of spectrum-planning guidance, vulnerability analysis, environmental analysis, and interference resolution. Support is available for wartime and contingency operations, joint training exercises, and for operations other than war such as disaster relief operations.

J5 Electromagnetic Environmental Effects (E3) Engineering Division – Provides E3 engineering support services to ensure optimal performance of military equipment, systems, and platforms in the operational electromagnetic environment without unacceptable mission

degradation. Ensure that E3 control and spectrum supportability are addressed during the acquisition process, in military standards, through training and awareness, and the development of analytical tools. Provide joint-service ordnance engineering services in the areas of ordnance testing, EMI surveys and investigations, and participation in joint exercises.

J8 Applied Engineering Division – Provides technical (E3) and spectrum engineering analysis and test support on a customer-funded basis. This includes support to DoD and other Federal Government organizations; to the private sector when it is in the interest of national defense per 10 U.S.C. 2539b; and to foreign entities when authorized by the Foreign Military Sales Process through the Defense Security Cooperation Agency.

JSB Defense Spectrum Relocation Management Activity (DSRMA) – Provides technical analysis support to the Office of the Secretary of Defense, Networks and Information Integration, related to the relocation of DoD spectrum-dependent devices out of the 1710-1755 MHz frequency band. DSRMA initiatives include a portal and analysis capability to handle requests from commercial Advanced Wireless Service providers seeking early access to this frequency band, and two other projects: the Spectrum Management Technology Initiative (SMTI) and the Spectrum Technology Testbed Initiative (STTI). The SMTI is focused on improving the mathematical algorithms used by spectrum managers to nominate frequencies to fit new spectrum-dependent devices into increasingly congested spectrum environments, especially for systems being relocated. The STTI is a federation of spectrum management simulation tools used to test the viability of proposed relocation solutions in a realistic operational environment.

JSC Operational Support Services and Products

Warfighting Unified Combatant Commands and Joint Task Force (JTF) Commanders services include:

- Review of operations plans for spectrum supportability, upon request.
- Joint Spectrum Interference Resolution (JSIR) support through analysis and deployment teams as necessary.
- SPECTRUM XXI software training and joint exercise support.
- Liaison and coordination support to Information Operations (IO) and Joint Information Operations Center organizations.
- Engineering support to the Joint Staff in Navigational Warfare and CIED matters.

Communications-Electronics (C-E) Planning products and services are provided to the Joint Staff, Unified Commands, JTFs, Military Departments, Defense Agencies, and directly to the warfighter, including:

- SPECTRUM XXI Frequency Nomination/Assignment/Allotment.
- Electronic Warfare (EW) deconfliction.
- Joint Restricted Frequency List (JRFL) creation and analysis.
- Interference Analysis.
- Propagation Predictions (MF-EHF).
- Communication System Performance Prediction.
- Radar Target Acquisition Coverage Prediction.
- Electromagnetic Compatibility Analyses in Support of Frequency Planning.
- Topographical Analyses.
- Joint Communications-Electronics Operating Instruction Planning/Preparation.
- Electromagnetic Environment Definition.

JSIR services are structured to have interference incidents resolved at the lowest possible level of the DoD component chain of command, using component organic resources to resolve interference incidents where possible. Interference reports are entered and available at www.intelink.sgov.gov/sites/jsir. Those incidents that cannot be resolved locally are referred up the chain of command, with resolution attempted at each level.

If the interference incident cannot be resolved by the affected DoD Component or the service engineering agency responsible for spectrum interference resolution, then it is referred to the JSC JSIR office for resolution. The JSC JSIR office will analyze and attempt to recommend corrective action for reported interference problems by first using JSC databases and analytical tools, and then, if needed, by providing personnel and equipment to perform on-site direction finding, equipment test, and problem solution. If the assistance is requested for electronic attack incidents, the JSC JSIR office will coordinate analysis, collection, and field support activities with the appropriate agencies.

The objective of the JSIR Team is to assist with the resolution of recurring EMI. The three-step resolution process for EMI events includes:

1. Identification, verification, characterization, and reporting.
2. Geolocation, analysis, developing courses of action, and corrective action recommendations.
3. Implementation and notification to user(s) and final closure reporting.

The deployable interference resolution teams have the capability to:

- Identify – through an analytical process using spectrum monitoring equipment, man portable and/or vehicle mounted, capable of capturing frequencies up to 40 GHz.
- Locate – by means of cutting edge Radio Frequency Direction Finding (RDF) technology utilizing portable, mobile and space based systems.
- Analyze - through investigation provided by a multiple resource reach back capability for research by many different RF disciplines to analyze DOD communications systems while providing situational awareness.

Command and Control (C2)-Protect services are provided through each of the following activities:

- Provision of databases on friendly force C2 system location and technical characteristics data for use in planning C2-protect. The databases cover DoD, US government, and civil communications, as well as radar, navigational aids, broadcast, EW, and identification systems. The databases are available on a quick reaction basis in a variety of formats and media to meet the needs of IO planners and spectrum managers.
- Assistance to the EW or IO officer in the development of the JRFL. The JSC provides an automated tool, SPECTRUM XXI, to assist in the development and management of the JRFL. The JSC has Unified Combatant Command support teams that deploy to the combatant command or JTF. The teams are available to prepare the JRFL or provide training and assistance in JRFL preparation. These teams are also available to provide assistance in spectrum management matters.
- Assistance in the resolution of operational interference and jamming incidents through the auspices of the JSIR Program.
- Provision of data on communications frequency and location data.
- Production of country studies. JSC Country Studies are published on the JSC website in support of Unified Combatant Command requirements. Each study provides information on civil telecommunications including: frequency management; broadcasting; telephone; data communications; aeronautical communications; maritime communications; and

transmission systems. Frequency allocations, assignments, histograms, and site location maps are also included. The frequency assignment data is provided in a spreadsheet compatible format and in vertical Standard Frequency Action Format (SFAF) compatible with SPECTRUM XXI.

Spectrum Regulatory Support services address the growth of commercial wireless services, such as Personal Communications Services, and has greatly increased the demand for spectrum and increased pressure for the government to relinquish portions of the spectrum to commercial interests. Continuing pressure to reallocate portions of the spectrum requires that the DoD have the ability to quickly assess the operational and economic impact of proposed reallocation legislation in order to defend critical DoD spectrum access. The JSC draws upon a collection of databases and experience with spectrum management to respond to ad hoc inquiries. In addition, the JSC is positioned to develop in-depth assessments of various reallocation proposals that will provide all levels of government with the information needed to make responsible reallocation decisions.

Leadership: The command billet of the center (O-6) rotates between the Army, Air Force, and Navy. The JSC Commander reports to the Director, Defense Spectrum Organization who in turn reports to the DISA Vice Director.

NIPR Website: http://www.disa.mil/jsc/
NIPR email: operations@jsc.mil

SIPR Website: http://jsc.disa.smil.mil
SIPR email: JSCOperations@disa.smil.mil

JWICS Website: http://jsc.ic.gov
JWICS email: operations@jsc.ic.gov

Updated October 2011

Joint Public Affairs Support Element (JPASE)

Mission: The Joint Public Affairs Support Element (JPASE) trains and maintains a public affairs professional capability to rapidly deploy as a team to assist the combatant commanders. The operational teams help to properly disseminate information to the public. The goal is for these professionals to provide counsel, operational planning and tactical execution of communication strategies as a function of joint military operations in support of national objectives. JPASE is located in the Joint Coalition Warfighting Center in Suffolk, VA. It is a subordinate command of U.S. Transportation Command's Joint Enabling Capabilities Command (JECC).

JPASE Mission Statement: The Joint Public Affairs Support Element (JPASE) provides a ready, rapidly deployable joint public affairs capability to facilitate establishment of joint force headquarters and to bridge capability gaps in response to developing crises or contingency operations. JPASE also provides joint public affairs training, through participation in the Joint Exercise Program, to better enable joint force commanders and their staffs to successfully meet evolving public affairs and information challenges in their respective theaters of operation.

JPASE is organized to provide direct support to specific combatant command requirements. It replaces the former, *ad hoc* method of assembling teams to provide support. This new organization facilitates concentration on the particular aspects of geography, culture and organization of a specific command, while gaining proficiency and understanding of the common operating tools and practices each command employs. On order, JPASE deploys to the regional Combatant Commands in support of emergent joint operations as a trained, equipped and ready joint public affairs force. Its first deployment was during Hurricane Katrina in 2005 and it has deployed teams to support joint operations twenty times since. Twenty three of JPASE's 25 military and civilian personnel, drawn from all services, are designated to support expeditionary operations.

Organization: JPASE is organized around two objective areas:

1. **Global Response Force Operations**
   - JPASE provides rapidly deployable, scalable, equipped and trained Joint Public Affairs capabilities to support emergent joint requirements.
2. **Training and Education**
   - JPASE provides PA training to enable Joint Force Commanders and their staffs to successfully meet continuously evolving information environment challenges in their respective theaters of operations.

Reserve Components Capability: A reserve joint public affairs unit (JPASE-R) supports and augments the active duty JPASE organization. It is trained and equipped to provide training and support for the active JPASE force during day-to-day operations and when it is deployed in support of emergent and contingency operations.

Updated: October 2011

This Page Intentionally Blank

Joint Information Operations Warfare Center (JIOWC)

Mission: The Joint Information Operations Warfare Center supports the Joint Staff in improving the Department of Defense's ability to meet combatant command information-related requirements, improving development of information-related capabilities, and ensuring operational integration and coherence across combatant commands and other DOD activities.

Functions:

- Joint IO Assessment
- Joint IO Force Development
- Joint Operations Security
- Joint Military Deception
- Coordinate and integrate DOD IO operational support for joint commanders

Capabilities:

- Provides IO Subject Matter Experts with special emphasis on Military Deception and Operations Security
- Maintains a cadre of intelligence professionals tightly focused on the IO problem set
- Maintains a habitual working relationship with the IO staffs of the combatant commanders and service elements
- Provides focused and tailored IO planning products

History and Subordination: The Joint Electronic Warfare Center (JEWC) was established by the Secretary of Defense in October 1980 and reported to the Joint Staff. In September 1994, the mission was expanded and the organization was renamed the Joint Command and Control Warfare Center (JC2WC). In 1998, as a result of the Defense Reform Initiative (DRI), the JC2WC was realigned from the Joint Staff to US Atlantic Command. The JC2WC mission was further expanded and resulted in redesignation as the Joint Information Operations Center (JIOC). In October 1999, the JIOC was realigned as a subordinate command of USSPACECOM. On 1 October 2002, the JIOC was realigned as a subordinate command to USSTRATCOM. In 2006 the JIOC was renamed the Joint Information Operations Warfare Command (JIOWC) and focused on operational IO planning and operations. Subsequently, the JIOWC was renamed the Joint Information Operations Warfare Center. On 1 October 2011, the JIOWC was reassigned under the Joint Staff as a Chairman's Coordinating Activity. The JIOWC Director reports to Joint Staff J3, through the Deputy Director Global Operations, J39 (DDGO).

Leadership: The Director of the JIOWC is a Defense Intelligence Senior Executive Service position that is filled by a competitive civil service selection process.

Location: The JIOWC is co-located with the Air Force Intelligence, Surveillance & Reconnaissance Agency and components of 24th Air Force at Lackland AFB, TX in San Antonio, TX.

SIPR Website: http://www.jiowc.smil.mil

Updated: October 2011

This Page Intentionally Blank

U.S. Strategic Command (USSTRATCOM)

U.S. Strategic Command (USSTRATCOM) is one of nine combatant commands in the Department of Defense. It is located at Offutt Air Force Base near Omaha, Neb. General C. Robert Kehler commands USSTRATCOM and serves as the senior commander of unified military forces from all four branches of the military assigned to the command. He is responsible for the global command and control of U.S. strategic forces to meet decisive national security objectives. USSTRATCOM provides a broad range of strategic capabilities and options for the President and Secretary of Defense. USSTRATCOM integrates and coordinates the necessary command and control capability to provide support with the most accurate and timely information for the President, the Secretary of Defense, other National Leadership and geographic combatant commanders, and serves as steward and advocate of the nation's strategic capabilities.

The mission of the U.S. Strategic Command is to detect, deter, and prevent attacks against the United States and our allies - join with the other combatant commands to defend the nation should deterrence fail.

The priorities of the Command are:

1. Deter nuclear attack with a safe, secure, effective nuclear deterrent force.
2. Partner with the other COCOMS to win today.
3. Respond to the new challenges in space.
4. Build cyberspace capability and capacity.
5. Prepare for uncertainty.

The Secretary of Defense directed the joint force to reorganize development and management of IO by assigning proponency for joint IO to the Joint Staff. Individual capability responsibility of Computer Network Operations and Electronic Warfare remain assigned to USSTRATCOM. The Chairman of the Joint Chiefs of Staff reorganized elements of the Joint Information Operations Warfare Center (JIOWC), previously assigned to USSTRATCOM. The JIOWC's Joint Electronic Warfare Division remains assigned to USSTRATCOM and the remaining elements of the JIOWC were aligned with the Joint Staff.

The Command, including components, employs more than 2,700 people, representing all four services, including DoD Civilians and contractors, who oversee the command's operationally focused global strategic mission. The command is organized under a modified J-code structure as follows:

> **J0 The office of the Commander and the staff support agencies** - establishes the goals, mission, vision and leadership of the command. To help the commander, the immediate staff also includes the deputy commander in chief and a group of special advisors.

J1 (Manpower and Personnel) - provides the United States Strategic Command with manpower and personnel advice, support, and execution of Command policies and procedures to ensure maximum readiness and sustainability of the total force as both a supporting and supported Command.

J2 (Intelligence) - delivers all-source intelligence while enabling the execution of assigned strategic deterrence, space, and cyberspace operations and Joint mission enablers; directs all intelligence-related support for the Commander; ensures unity of intelligence effort across the Command; and advocates for Command intelligence requirements.

J3 (Global Operations) - coordinates the planning, employment and operation of DoD strategic assets and combines all current operations, global command and control, and intelligence operations. Subdivisions within the J3 include Combat and Information Operations, Intelligence, Current Operations, Logistics, Joint Exercise and Training, and C4 Systems.

J4 (Logistics) - provides integrated logistics capabilities enabling USSTRATCOM and components to achieve desired global effects.

J5 (Plans and Policy) - develops and refines strategies, policies, concepts, guidance, and plans to focus and synchronize USSTRATCOM planning across the command's mission areas in collaboration with the command's staff and components, other combatant commanders, the Joint Staff, OSD, and other US Agencies. With a global perspective, develops commander's estimates; intent; strategic themes, actions, and responses; and policy positions to ensure command operations and activities are integrated with other combatant commands and elements of national power to accomplish USSTRATCOM's global missions and provide synchronized support to combatant commands and agencies.

J6 (C4 Systems) - provides and assures global-integrated Command, Control, Communications, and Computer Systems (C4) capabilities for US Strategic Command to execute support of full spectrum global strike, space, and information operations. Responsible for management of over $20B of on-orbit communications assets. Translates DoD and JCS policy into capabilities. Directorate consists of 457 military, civilian, contractors, and a $103M/year budget.

J7 (Joint Exercises and Training) - manages USSTRATCOM Commander's Joint Training Program and Exercise Program in order to ensure readiness to perform the Command Missions. Provides modeling and simulation support for exercises and training events to the Joint Chiefs of Staff (JCS), Combatant Commands, and other Major Commands (MAJCOMs). Manages the Joint Lessons Learned Program. Augments the battle staff during a crisis.

J8 (Capability and Resource Integration) - identifies, analyzes, and advocates for capabilities and resources to accomplish US Strategic Command's assigned missions of strategic deterrence, global strike, space operations, information operations, integrated missile defense, combating weapons of mass destruction, and global command, control, intelligence, surveillance, and reconnaissance. Develops and manages current and future year financial plans.

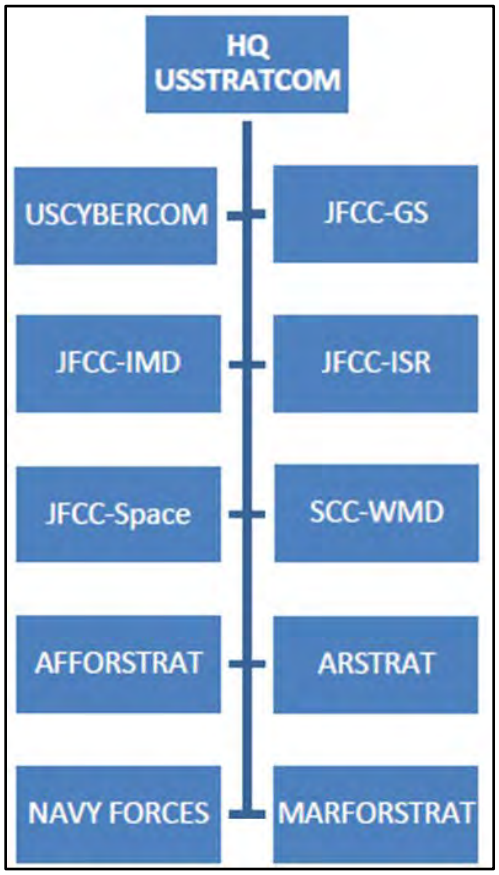
J9 (Mission Assessment and Analysis Directorate) - conducts operational and strategic assessments and leverages industry, academia, US Government agencies, and Allies to improve USSTRATCOM's warfighting ability. The Assessments Division leads command operational and strategic assessment activities that inform

Commander's decision-making regarding his assigned Unified Command Plan (UCP) missions and progress toward achieving Guidance for Employment of the Force (GEF) end states.

USSTRATCOM exercises command authority over various task forces and service components in support of the command's mission. During day-to-day operations, service component commanders retain primary responsibility for maintaining the readiness of USSTRATCOM forces and performing their assigned functions. Their primary function is to provide organized, trained, and equipped forces for employment when called upon to support USSTRATCOM's global mission.

As the Department of Defense's key advocate for global capabilities, the command has extensive ties with defense agencies, the Department of Energy's national laboratories, and other sources of support. Through its many contacts and interagency relationships, the command facilitates planning, enhances information sharing between the military and other government agencies and streamlines decision making.

USSTRATCOM Functional Components, Service Components, Task Forces, and subunified Command:



USSTRATCOM exercises command authority over three joint functional component commands (JFCCs) responsible for day-to-day planning and execution of primary mission areas: Strategic Deterrence/Nuclear Operations, and Space Operations, a subunified command for the Cyberspace Operations mission area; as well as performing a global synchronization role in:

Missile Defense, Surveillance and Reconnaissance, and combating weapons of mass destruction.

United States Cyber Command (USCYBERCOM) - plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries. USCYBERCOM is a subunified command of USSTRATCOM.

JFCC Global Strike (JFCC GS) - optimizes planning, integration, execution and force management of assigned missions of deterring attacks against the U.S., its territories, possessions and bases, and should deterrence fail, by employing appropriate forces.

JFCC Integrated Missile Defense (JFCC IMD) - develops desired characteristics and capabilities for global missile defense operations and support for missile defense. Plans, integrates and coordinates global missile defense operations and support (sea, land, air and space-based) for missile defense.

JFCC Intelligence, Surveillance and Reconnaissance (ISR) (JFCC ISR) - plans, integrates and coordinates intelligence, surveillance and reconnaissance in support of strategic and global operations and strategic deterrence. Tasks and coordinates ISR capabilities in support of global strike, missile defense and associated planning.

JFCC Space (JFCC Space) - optimizes planning, execution, and force management, as directed by the commander of USSTRATCOM, of the assigned missions of coordinating, planning, and conducting space operations.

USSTRATCOM Center for Combating Weapons of Mass Destruction (SCC- WMD) - plans, advocates and advises the commander, USSTRATCOM on WMD-related matters. Provides recommendations to dissuade, deter and prevent the acquisition, development or use of WMD.

For More information please visit www.stratcom.mil

Updated: October 2011

U.S. Cyber Command (USCYBERCOM)

On June 23, 2009, the Secretary of Defense directed the Commander of U.S. Strategic Command (USSTRATCOM) to establish USCYBERCOM. The command achieved Initial Operational Capability (IOC) on 21 May 2010 and attained Full Operational Capability (FOC) on 31 October 2010.

Formal Command Name: U.S. Cyber Command (USCYBERCOM or CYBERCOM)

Commander: General Keith B. Alexander

Mission: USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.

Focus: USCYBERCOM will fuse the Department's full spectrum of cyberspace operations and will plan, coordinate, integrate, synchronize, and conduct activities to: lead day-to-day defense and protection of DoD information networks; coordinate DoD operations providing support to military missions; direct the operations and defense of specified DoD information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations. The command is charged with pulling together existing cyberspace resources, creating synergy that does not currently exist and synchronizing war-fighting effects to defend the information security environment.

USCYBERCOM will centralize command of cyberspace operations, strengthen DoD cyberspace capabilities, and integrate and bolster DoD's cyber expertise. Consequently, USCYBERCOM will improve DoD's capabilities to ensure resilient, reliable information and communication networks, counter cyberspace threats, and assure access to cyberspace. USCYBERCOM's efforts will also support the Armed Services' ability to confidently conduct high-tempo, effective operations as well as protect command and control systems and the cyberspace infrastructure supporting weapons system platforms from disruptions, intrusions and attacks.

Organization and Forces: USCYBERCOM is a sub-unified command subordinate to USSTRATCOM. Service elements include:

- USA – Army Cyber Command (ARFORCYBER/2nd Army)
- USAF – Air Force Cyber Command (AFCYBER/24th AF)
- USN – Fleet Cyber Command (FLTCYBERCOM/10th Fleet)
- USMC – Marine Forces Cyber Command (MARFORCYBER)

Point of Contact: U.S. Cyber Command Public Affairs (301)688-6584
http://www.defense.gov/cyber

Updated: October 2011

This Page Intentionally Blank

U.S. Special Operations Command (USSOCOM)

USSOCOM is one of the nine U.S. unified commands under DOD. It organizes, trains, equips and provides special operations forces to Geographic Combatant Commanders, American Ambassadors and their country teams. USSOCOM commands and controls all US-based SOF from all four services. It also develops SOF-specific tactics, techniques, procedures, and doctrine, and conducts research, development, and acquisition of SOF-peculiar equipment. USSOCOM ensures its forces are trained and ready to respond to the call from the President, Secretary of Defense and the geographic combatant commanders as necessary.

Mission. USSOCOM provides fully capable Special Operations Forces to defend the United States and its interests. Synchronizes plans and planning of global operations against terrorist networks.

Special operations are operations conducted in hostile, denied, or politically sensitive environments to achieve military, diplomatic, informational, and/or economic objectives employing military capabilities for which there is no broad conventional force requirement. These operations often require clandestine or discreet capabilities. Special operations are applicable across the range of military operations. They can be conducted independently or in conjunction with operations of conventional forces or other government agencies and may include operations by, with, or through indigenous or surrogate forces.

Special Operations Forces Core Operations

- **Counter-proliferation of weapons of mass destruction (CWMD)** - actions taken to locate, identify, seize, destroy or capture, recover, and render such weapons safe.
- **Counterinsurgency (COIN)** - those military, paramilitary, political, economic, psychological and civic actions taken by a government to defeat insurgency.
- **Counterterrorism (CT)** - measures taken to prevent, deter, and respond to terrorism.
- **Foreign Internal Defense (FID)** - providing training and other assistance to foreign governments and their militaries to enable the foreign government to provide for its country's national security.
- **Stability Operations** - military missions, tasks and activities conducted outside the U.S. in coordination with other instruments of national power to maintain or reestablish a safe and secure environment and to provide essential government services, emergency infrastructure reconstruction and humanitarian relief.
- **Unconventional Warfare (UW)** - operations conducted by, through, and with surrogate forces that are organized, trained, equipped, supported, and directed by external forces.
- **Support to Major Operations and Campaigns** - operations in support of conventional forces as part of a GCC operation or campaign involving major combat forces.

Special Operations Forces Core Activities

- **Civil Affairs Operations (CAO)** - activities that establish, maintain or influence relations between U.S. forces and foreign civil authorities and civilian populations to facilitate U.S. military operations.
- **Direct Action (DA)** - short-duration strikes and other small scale offensive actions taken to seize, destroy, capture, recover or inflict damage in denied areas.
- **Hostage Rescue and Recovery** - sensitive crisis response missions that include offensive measures taken to prevent, deter, preempt and respond to terrorist threats and incidents, including recapture of U.S. facilities, installations and sensitive material.
- **Military Information Support Operations (MISO)** - operations that provide truthful information to foreign audiences that influence behavior in support of U.S. military operations.
- **Security Force Assistance (SFA)** - unified actions by joint, interagency and the multinational community to sustain and assist host nation or regional security forces in support of a legitimate authority.
- **Special Reconnaissance (SR)** - acquiring strategic and operational information concerning the capabilities, intentions and activities of an enemy.
- **Activities specified by the President or Secretary of Defense.**

IO Core and Related Capabilities within USSOCOM Purview:

- **Military Information Support Operations (MISO).** A vital part of the broad range of U.S. political, military, economic, and information activities used by the U.S. government to secure national objectives, MISO disseminates truthful information to foreign audiences in support of U.S. policy and national objectives. Used during peacetime, contingency operations, and declared war, these activities are not a form of force but are force multipliers that use nonviolent means in often violent environments. Persuading rather than compelling physically, they rely on logic, fear, desire or other mental factors to promote specific emotions, attitudes or behaviors. The ultimate objective of U.S. military information support operations is to convince target audiences to take action favorable to the United States and its allies. The importance and effectiveness of military information support operations has been underscored during OPERATIONS ENDURING FREEDOM and IRAQI FREEDOM.
- **Civil Affairs (CA).** CA units support military commanders by working to minimize the effect of civilians in the battle space and by coordinating with civil authorities and civilian populations in the commander's area of operations to lessen the impact of military operations on them during peace, contingency operations, and declared war. Civil Affairs forces support activities of both conventional and SOF, and are capable of assisting and supporting the civil administration in their area of operations. Long after the guns have fallen silent, the men and women of Civil Affairs continue to provide assistance to foreign governments, and to stabilize regions in turmoil.

Components. USSOCOM has four component commands and one sub-unified command:

1. **U.S. Army Special Operations Command (USASOC).** Located at Ft. Bragg, North Carolina. USASOC's mission is to organize, train, man, equip, educate, maintain combat readiness, and deploy assigned active duty and National Guard units of the Army

Special Operations Force. Their mission is to accomplish special operations, military information support operations, and civil affairs operations. Their forces include:

1. 4th MISO Group (Airborne) (4th MISOG)
2. 8th MISO Group (Airborne) (8th MISOG)
3. 95th Civil Affairs Brigade (Airborne)
4. United States Special Forces Command (Airborne).
5. John F. Kennedy Special Warfare Center and School.
6. 75th Ranger Regiment
7. United States Army Special Operations Aviation Command
   - 160th Special Operations Regiment (Airborne)
8. 528th Sustainment Brigade (Airborne)

2. **Naval Special Warfare Command (NAVSPECWARCOM).** Located at Naval Amphibious Base, Coronado, CA. The mission of NAVSPECWARCOM is to organize, train, man, equip, educate, maintain combat readiness, and deploy assigned forces in support of joint and fleet operations worldwide. SEAL Teams are maritime, multipurpose combat forces organized, trained and equipped to conduct a variety of special operations missions in all operational environments and threat conditions. SEAL mission areas include direct action, counter-terrorism, special reconnaissance, foreign internal defense, information warfare, security assistance, counter-drug operations, and hydrographic reconnaissance.
3. **Air Force Special Operations Command (AFSOC).** Located at Hurlburt Field, FL. It provides Air Force Special Operations Forces to conduct and support global special operations missions. AFSOC's contribution to Information Operations is specifically in the form of the 193d Special Operations Wing, Air National Guard. The wing operates the EC 130 "Commando Solo", which can broadcast television and radio programs directly to foreign audiences.
4. **Marine Corps Forces Special Operations Command (MARSOC).** Located at Camp Lejuene, NC. Activated February 2006, its primary mission is to organize, man, train and equip Marine Special Operations Forces. The MARSOC subordinate elements provide training to foreign militaries, conduct specified special operations missions like special reconnaissance, engage in direct action, provide intelligence support, coordinate supporting fires and provide logistical support to special operations task forces.
5. **Joint Special Operations Command (JSOC).** A sub-unified command of USSOCOM. JSOC provides a joint headquarters to study special operations requirements, ensures interoperability and equipment standardization, develops joint special operations plans and tactics, and conducts joint special operations exercises and training.

Location Address and Contact Information: Headquarters, United States Special Operations Command (HQ, USSOCOM)

Headquarters, USSOCOM
7701 Tampa Point Boulevard
MacDill Air Force Base, FL 33621

Public Affairs Office: (813) 826-4600

Website: http://www.socom.mil/

Updated: October 2011

This Page Intentionally Blank

Joint Forces Staff College – Information Operations Program

The Joint Forces Staff College (JFSC) was established in 1946 to better equip personnel from all of the services to function in the modern joint and combined warfare environment. It pre-dates the creation of the unified Department of Defense and is the successor of the Army and Navy Staff College, established in 1943 for the same purpose. The college is located at the U.S. Naval Base, Norfolk, VA.

IO Education at JFSC. Department of Defense Instruction (DODI) 3608.12, "Joint Information Operations (IO) Education", (4 November 2005) specifies that, "Joint Forces Staff College [will] develop and conduct a Joint IO planners course to prepare students to integrate IO into plans and orders on joint warfighting staffs." The College also offers a Joint IO orientation course. Both are conducted by the Information Operations Division of the Joint Command, Control & Information Operations School (JC2IOS) and are outlined below.

1. Joint IO Orientation Course (JIOOC)
A one week course with the objective to educate and train U.S. Government (USG) personnel in the military grades of Lieutenant/Captain (O-3) to Captain/Colonel (0-6) and civilian equivalents in the basics of joint Information Operations (IO). Primary emphasis is at the Combatant Command level. The course focuses on teaching joint IO doctrine and DoD IO policy guidance as they apply to the operational level of joint warfare. It is particularly relevant to those serving in support of IO cells and other staff positions that require a basic knowledge of Joint IO. If IO planning skills are desired, then the student should take the Joint Information Operations Planner's Course (JIOPC).

JIOOC gives students a common baseline of IO knowledge upon which to build practical skills and abilities to employ IO tools and techniques. In this one-week course, students are exposed to four blocks of instruction: Strategy; Intelligence support; IO Capabilities (Core, Supporting and Related); and Organization, Training, and Equipping. Each block of instruction includes a combination of instructor lecture, guest speaker presentations, guided discussions and/or panel discussions.

2. Joint Information Operations Planner's Course (JIOPC)
A four-week course for the purpose of establishing a common level of understanding for IO planners and IO capability specialists, between the ranks of 0-4 through 0-6, and DoD Civilian equivalents, who will serve in joint operational-level IO billets. *This course is required for Joint IO Career Force personnel assigned to a combatant command or JTF staff* (See CJCSM 1630.01, *Joint Information Operations Force*, 16 March 09).

The objective of the JIOPC is to educate and train to plan, integrate, and synchronize IO into joint operational-level plans and orders. The school accomplishes this through class presentations, guest lectures, case studies, and practical exercises in a joint seminar

environment. Students will be assigned to a working group consisting of approximately eight to ten individuals led by a faculty mentor. The course focuses on the following learning areas:

- Joint Operational Planning Process (JOPP)
- Joint Intelligence Preparation of the Environment (JIPOE)
- Information Operations (IO) Planning
- Interagency Planning & Coordination

Throughout the course the students use traditional planning methodologies within the joint planning community. The course is based upon joint doctrine that is reinforced, when necessary, by a compilation of various tactics, techniques, and procedures from throughout the department of defense.

The JIOPC is only taught in residence at the Joint Forces Staff College.

The JC2IOS Division of JFSC also offers Mobile Training Teams (MTT's) to commands needing orientation training. MTT's are funded by the host.

For information regarding the JFSC Information Operations Division, contact JC2IOS-IO@jfsc.ndu.edu or at 757-443-6336/6333 (DSN: 646).

Web Site: http://www.jfsc.ndu.edu/

Reviewed: October 2011

Information Operations Center for Excellence
Naval Postgraduate School

The Naval Postgraduate School (NPS) is located in Monterey, CA and is the successor to the Postgraduate Department of the US Naval Academy, established at Annapolis, MD prior to World War I. Congress established the school as a full degree-granting institution in 1945, and it moved to its present location in 1951. The present student body numbers approximately 1,800, with representatives from all service branches, and the services of more than 25 allied nations. It grants degrees at the master's and doctorate levels.

Information Operations Center for Excellence. The President, NPS was tasked by Department of Defense Instruction (DoDI) 3608.12 Joint Information Operations (IO) Education, dated 4 November 2005, to "Establish the DoD IO Center of Excellence."

The IO Center for Excellence (IOCfE) functions under the sponsorship of the Under Secretary of Defense for Policy to inform and support the development of innovations in IO related policy, technology, research and education.

The IOCfE exists to:

- advance the goal of information operations as a core military competency
- support the DOD commitment to transform our military capabilities
- provide avenues for research for information operations, irregular warfare and unconventional thought

Information Operations Education at NPS

1. Doctor of Philosophy in Information Sciences (Curriculum 474). The Department of Information Sciences at the Naval Postgraduate School will award the Doctor of Philosophy in Information Sciences degree as a result of meritorious and scholarly achievement in a particular field of information sciences (IS). This program includes course work, scholarly socialization, written and oral examinations, research, and a written dissertation. A candidate must exhibit scholarly application to the entire course of study, achieve a high level of scientific advancement, and establish ability for original investigation leading to the advancement of fundamental knowledge.

IS broadly encompasses the design, implementation, use, promotion and evaluation of organizations, processes and systems associated with knowledge, information, data and communication. It includes areas of concentration in information systems, information technology, information warfare, information operations, and command and control.

The Ph.D. in Information Sciences prepares scholars to conduct original research that contributes new knowledge in the domain of information systems, information technology, information warfare, information operations, or command and control. With such ability to conduct original research and contribute new knowledge, the IS Ph.D. helps to prepare scholars also to teach effectively.

Website: Information on Naval Postgraduate School's PhDIS can be obtained at the following site: http://www.nps.edu/Academics/GeneralCatalog/414.htm#o435.

2. Master of Science in Joint Information Operations (Curriculum 698). The Joint Information Operations curriculum educates military personnel and civilian officials in the strategic and operational dimensions of information and its use as an instrument of statecraft. Graduates will be able to employ information in support of full-spectrum dominance by exploiting the growing worldwide dependence on information systems, and by capitalizing on near real-time global dissemination of information to affect adversary decision cycles, with the goal of achieving information superiority for the United States.

The curriculum is designed for both the specialist who will be assigned to an information operations position and the generalist who will be assigned to an operations directorate. The curriculum includes a core of military art and operations, the human dimension of warfare (psycho-social), analytical methods, and a customized elective sequence designed for each student. Additionally, each student will have an elective sequence designed to further develop an in-depth understanding of joint information operations. Finally, each student will write a thesis relevant to the field of information operations.

Website: Information on the JIO Curriculum can be obtained at the following site: http://www.nps.edu/Academics/GeneralCatalog/414.htm#o425.

3. Master of Science in Information Systems and Operations (Curriculum 356). This curriculum, offered through the Information Sciences Department, is a war-fighter oriented, in-residence MS degree, program that will provide fundamental graduate education to integrate information technologies, command and control processes, and IO methods and elements into innovative operational concepts for Information Operations in the context of Network Centric Warfare.

- The Information Systems & Operations graduate will be able to:
- Innovatively create IO strategies and policies.
- Establish agile organizational structures and decision processes responsive to real time mission and situation requirements.
- Understand information technology and systems as enabling the acquisition of information and knowledge superiority leading to effective development and performance of information operations.
- Integrate technology, organization, policy and strategy into an Information Operations framework useful in both deliberate and crisis planning across the range of military operations;
- Identify and solve significant information operations problems and communicate the results in written reports and command briefings.

Website: Information on Naval Postgraduate School's ISO program can be obtained at the following site: http://www.nps.edu/Academics/GeneralCatalog/414.htm#o429

4. Master of Science in Information Warfare Systems Engineering (Curriculum 595). Graduates of this curriculum are thoroughly knowledgeable in Information Operations (IO) and Information Warfare (IW). They receive a Master of Science in Information Warfare Systems Engineering (MSIWSE) degree that provides the services with officers who are well versed in the technical, theoretical, and operational aspects of interdisciplinary IO/IW as they relate to joint mission objectives in modern warfare. This curriculum is sponsored by Commander, Naval Network Warfare Command, Information Operations Directorate.

Website: Information on Naval Postgraduate School's MSIWSE program can be obtained at the following site: http://www.nps.edu/Academics/GeneralCatalog/414.htm#o436.

5. Master of Science in Cyber Systems and Operations (Curriculum 326). In response to a rapidly changing operational environment NPS, under the guidance of Navy N2/N6, has developed a new curriculum in Cyber Systems and Operations (CSO). The objective of this curriculum is to provide the services with officers able to address the broad range of cyberspace operations: computer network attack, defense, and exploitation; cyber analysis, operations, planning and engineering; and cyber intelligence operations and analysis.

The CSO degree is comprised of eighteen courses, all of which are intended to provide a coherent, logical sequence of educational objectives associated with operations in the Cyber domain. This program will complement the Information Systems Operations, which focuses on operations in the Information Domain.

6. Information Systems and Operations (ISO) Academic Certificate Program. NPS offers this certificate program in an asynchronous online mode. It is a part of its Master of Science (MS) degree in Information Systems and Operations (ISO) offered through the Information Sciences Department, The certificate program consists of four courses given via Distributed Learning (DL). These four courses are:

SS3011 - Space Technology and Applications
IO3100 - Information Operations
IS3502 - Computer Networks: Wide Area/Local Area (Intro to Information Systems Networks)
CC3000 - Intro to Command, Control, Communication, Computer and Intelligence Systems in DoD
ISO Academic Certificate Website: http://www.nps.edu/DL/Cert_Progs/ISO.asp

Information Operations Research, Conferences, Publications, and other Activities at NPS

In addition to the certificate and degree programs above, faculty and students at NPS conduct unclassified and classified research and field experimentation in technologies and concepts that are related to information operations/information-related capabilities, often in partnership with other academic institutions, national and regional research institutions and laboratories, defense industry, and military commands.

Since 2005 NPS has held or led a series of conferences and other activities dealing with the nature of operations in the post-9-11 world and the role information plays in this world. Subjects have run from "Cyber Conflict, International Cooperation and Deterrence" and "Understanding Terrorist Networks and Organizations" to "NPS-Salinas Counter-gang Collaboration" to "Information Operations and Force Transformation." Sponsors for these conferences include OSD, SOCCENT, and RRTO, among others.

NPS faculty author and NPS supports publication of relevant scholarly books and articles in the information strategy and warfare arena.

Updated: August 2011

This Page Intentionally Blank

Service Organizations

This section includes a description of the following organizations:

- **Army Cyber Command**
- **Army – 1st Information Operations Command (1st IO Cmd)**
- **Army Reserve Information Operations Command (ARIOC)**
- **United States Army Information Proponent Office (USAIPO)**
- **Marine Corps Information Operations Center**
- **Navy Information Operations Organizations**
- **Air Force Intelligence, Surveillance and Reconnaissance Agency**
- **Headquarters 24th Air Force**
    - **624th Operations Center**
    - **67th Network Warfare Wing**
    - **688th Information Operations Wing**
    - **689th Combat Communications Wing**

This Page Intentionally Blank

Army Cyber Command/2nd Army

With the establishment of Army Cyber Command on 1 October 2010, the Army brings unprecedented unity of effort and synchronization of all Army forces operating in cyber-space. U.S. Army Cyber Command is the Army's service component in support of U.S. Cyber Command, a sub-unified command under U.S. Strategic Command.

Mission. U.S. Army Cyber Command plans, coordinates, integrates, synchronizes, directs, and conducts network operations and defense of all Army networks; when directed, conducts cyberspace operations in support of full spectrum operations to ensure U.S./Allied freedom of action in cyberspace, and to deny the same to our adversaries.

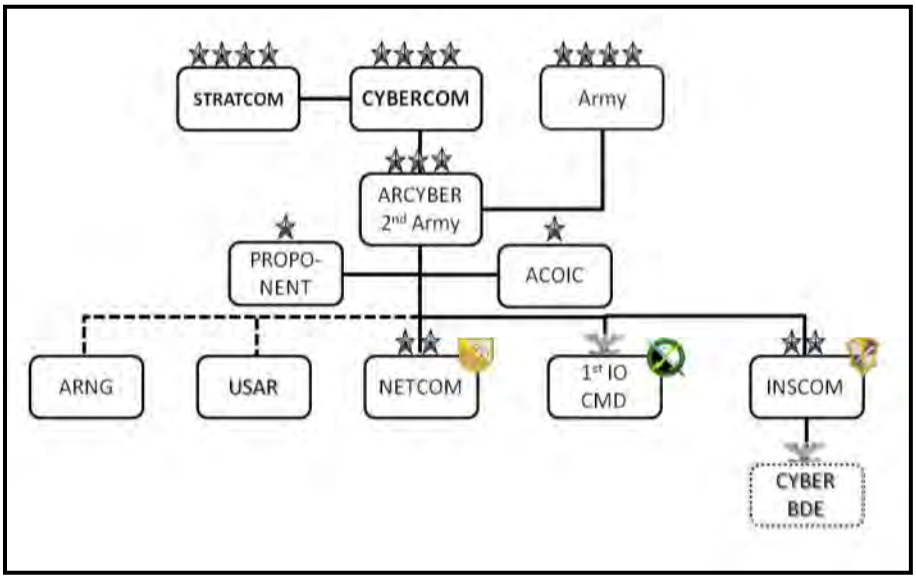
Roles. Army Cyber Command is the Army's proponent for cyberspace operations to improve all aspects of Army doctrine, organization, training, materiel, leadership, personnel, and facilities related to cyberspace operations.

- Serve as service component to US Cyber Command
- Train, organize and equip - Provide trained & ready forces
- Defense of all Army networks
- Proponency for Army Cyber … develop requirements
- Develop Army cyberspace capabilities and capacities
- Integrate cyberspace into planning and exercises
- Prepare to act as a cyber Joint Task Force Commander
- "Operationalize" cyber for the Army

Organization. U.S. Army Cyber Command has more than 21,000 Soldiers, DA Civilians and Contractors working across the globe conducting a full range of cyberspace operations - 24/7/365.

Army Cyber Command is a unified operations center responsible for all Army networks supported by:

- U.S. Army Network Enterprise Technology Command (NETCOM)
- U.S. Army Intelligence and Security Command (INSCOM)
- 1st Information Operations Command (Land)



Army Cyber Command Organization Chart

Army Cyber Vision 2020. A Professional team of elite, trusted, precise and disciplined warriors defending Army networks, providing a full range of dominant effects in and through cyberspace, enabling Mission Command and ensuring a decisive global advantage.

The Army must fundamentally transform cyber in order to meet the challenges of the 2020 strategic environment. By 2020, the Army will need to have achieved three critical thresholds for cyber:

- Integrated Cyber Capabilities
  - Army Cyber Warriors — integrated in cyber organizations & staffs
  - Full range of cyber operations are routine and pervasive
  - Nested with Joint Global, Expeditionary Cyber Constructs
- Achieve Cyber Domain Superiority
  - Cyberspace ops —seize, retain, & exploit the initiative
  - Seek the same level of freedom to operate that Army forces achieve in the Land domain
- Ensure Mission Command
  - Mission Command is enabled by cyber-space capabilities
  - Cyberspace Ops & Mission Command are inherently linked
  - Integrating construct for cyber-related ops & capabilities

Army Cyber 2020 Strategic Plan. The Army Chief of Staff directed ARCYBER to conduct a comprehensive assessment of Army cyber operations. This assessment led to the Army Cyber 2020 Strategic Plan, consisting of three Lines of Effort and three Enabling Activities.

Line of Operation #1 - Operationalize Cyber: Army Cyber Command will leverage and integrate current and future capabilities across the physical, informational, and cognitive dimensions of the information environment ensuring optimal effects in the cyberspace domain, as well as, enabling effects in the air, land, sea, and space domains.

- **Major Objectives**
  - Conduct Cyberspace Operations to Ensure Mission Command
  - Improve Intelligence Support to Cyberspace Operations
  - Conduct Intelligence Driven Integrated Cyberspace Operations
  - Streamline Army Cyberspace Command and Control
  - Build and Operate a Defensible Enterprise Network
  - Expand Army Critical Infrastructure Protection into the Cyber Domain
  - Change the Cultural View of Cyberspace Operations to that of a Contested Operational Domain
  - Develop a "World-Class" Cyber Opposing Force
  - Integrate Cyberspace and Information Operations into All Plans and Exercises
  - Enhance IO Support to Warfighters

Line of Operation #2 - Grow Army Cyberspace Capacity and Capabilities: As the Army's force modernization proponent for cyberspace operations, Army Cyber Command's proponent office will define the required force structure, develop critical doctrine and concepts, and integrate cyberspace operations into the Army's institutional processes in order to ensure superiority in the new cyberspace domain.

- **Major Objectives**
  - Determine and Prioritize Cyberspace Requirements for TAA and POM
  - Integrate Cyberspace Operations into Institutional Training
  - Develop the Future Cyber Force
  - Develop Capstone Cyberspace Doctrine and Concepts
  - Develop a World-class Cyberspace Proponent

Line of Operation #3 - Recruit, Develop, and Retain Cyber Professionals: While technology plays an important role in the cyberspace domain it is the cyber professionals, not the technology that will win on the 21st century's battlefields.

- **Major Objectives**
  - Determine and Prioritize Cyberspace Personnel Requirements
  - Develop the Future Cyber Warrior
  - Integrate Reserve Component Cyberspace Professionals into Total Army Solutions

Enabling Activities:

- People as a Priority
- Strategic Communications
- Build Headquarters Functional Capacity

Location. U.S. Army Cyber Command is located at Fort Belvoir, Va. with staff at Fort Meade, MD.

Army Cyber Command/2nd US Army
8825 Beulah Street Room GF10
Fort Belvoir, VA 22060-5246
www.arcyber.army.mil/

Updated: October 2011

This Page Intentionally Blank

Army – 1st Information Operations Command (1st IO Cmd)

Mission: 1st Information Operations (IO) Command (Land) provides IO support to the Army and other Military Forces through deployable IO support teams, IO reachback planning and analysis, and the synchronization and conduct of Army Computer Network Operations (CNO) in coordination with other CNO and Network Operations stakeholders, to operationally integrate IO, reinforce forward IO capabilities, and to defend Cyberspace in order to enable IO throughout the Information Environment.

Tasks:

1. Organize, train, equip and deploy mission capable IO Support Teams to provide IO planning and execution support or to conduct IO assessments as directed.
2. Provide IO planning plus operational, technical, and intelligence analysis reachback support to deployed IO support teams and supported commands.
3. Provide specialized IO and Cyber training support to LCCs, Army Commands, other Service Commands, Joint Forces, Agencies, Activities, Allies and Partners as directed.
4. Plan and conduct IO support to Army and Joint Cyberspace Operations in coordination with Cyberspace Operations stakeholders to defend Cyberspace and to enable other Information Operations as directed.
5. Operate the Army's World Class Cyber OPFOR to provide supported commanders an expert, agile, interactive adversary during exercises, training, and leader development.
6. Provide IO support for the assessment of force readiness and capabilities of Land Component Forces to accomplish their assigned missions as directed.
7. Develop and promote processes and procedures to ensure IO interoperability with Joint Forces, other Services, Inter-agencies, Allies and Partners.
8. Operate and maintain the Army's Operations Security (OPSEC) Support Element.
9. Provide IO support team training and evaluation standards to the Theater IO Groups.

As the single Army Active Component organization dedicated to IO, 1st IO Cmd is responsible for providing IO support to the warfighter in planning, synchronizing, de-conflicting, executing, and assessing IO. The Command supports warfighting and other commanders in conflict, other contingency operations, garrison, and in field training exercises and experiments. 1st IO Cmd operates with and across each of the IO competencies to gain an advantage through coordinated use of multiple capabilities to affect the Information Environment. 1st IO Cmd deploys IO Support Teams that provide IO planning, World Class Cyber OPFOR support, vulnerability assessments, OPSEC awareness, specialized training, Cyberspace Operations planning support, and specialized technical support. Additionally, 1st IO Cmd provides IO reachback capability to deployed teams and to the operational and tactical staffs of deployed forces, as directed.

Subordination: 1st IO Cmd is a major subordinate command to the U.S. Army Intelligence and Security Command (INSCOM) but is under the Operational Control and tasking of Army Cyber Command/2d US Army.

Leadership: The Commander of 1st IO Cmd is an Army Colonel who is qualified as a functional Area 30, Information Operations Officer. Battalion Commanders and key Brigade and Battalion staff are a mixture of FA-30, FA-53, Military Intelligence, Signal Corps, and other Branches and Functional Areas that represent the diverse skills and multi-component nature of the Command and its missions.

Location: The 1st IO Cmd is located at Ft. Belvoir, VA within the INSCOM HQs building. 1st IO Cmd has liaison positions established at the Pentagon, NSA, CAC, USAIOP/EWP, Joint Information Operations Warfare Center/Air Force IO Command, US Army Special Operations Command at Fort Bragg, USCENTCOM, and the National Air and Space Intelligence Center. 1st IO Cmd provides man, train, and equip support to Army Cyber Command's six Regional Computer Emergency Response Teams (RCERTs), which are collocated with each of the Army Service Component Commands.

Website: http://www.1stiocmd.army.mil/

Updated: October 2011

Army Reserve Information Operations Command (ARIOC)

Mission: On order, ARIOC conducts Computer Network Operations (CNO) in support of Army and Joint Commands to achieve information superiority of cyberspace.

Tasks:

- Organize, train, equip and deploy mission support teams (MST) to conduct planning, intelligence support and analysis, synchronization, and integration of Army CNO capabilities into full spectrum operations. ARIOC conducts cyber counter-reconnaissance, cyber-strategic reconnaissance, incident handling & response, and computer defense and assistance program (CDAP) augmentation in support of the 1st IOC (L) Army Computer Emergency Response Team (ACERT) and Regional Computer Emergency Response Team (RCERT) SWA mission. The command monitors the Defense Research and Engineering Network (DREN), deploys Vulnerability Assessment Teams (VAT), and supports the Army Net Risk Assessment Mission.
- Operates the secure, stand-alone ARIOC Cyber range. This network is used for CNO analysis, doctrine development, exercise support, training, certification and validation of cyber warrior skill sets. This network facilitates ARIOC participation in Joint level exercises with the JFCOM Joint IO Range.
- Develops, promotes policies, procedures and processes to integrate cyberspace operations (CO) into operations of the Army Reserve, reserve components of other services, inter-agencies and allies.
- The Army Reserve IO Command (ARIOC) applies the civilian acquired IT skills, knowledge and abilities of its citizen-soldiers to support Army and Joint Cyberspace requirements of the 21st century. ARIOC deploys experienced, skilled IO teams and individuals to augment Army & Joint capabilities in full spectrum operations.

Subordination: The ARIOC is a subordinate unit of the U.S. Army Reserve Joint & Special Troops Support Command (USARJSTSC), Fort Douglas, UT. ARIOC receives its operational tasking through the Army G-3 (Director of Operations, Readiness and Mobilization) and Forces Command (FORSCOM).

Leadership: The Commander of the ARIOC is an Army Reserve Colonel (O-6).

Location: ARIOC HQ is in Adelphi, MD at the Army Research Lab, Phone: S3 - 301.394.1190 or DSN 290-1190, DCDR - 301.394.1144 or DSN 290-1144.

Updated October 2011

This Page Intentionally Blank

United States Army Information Proponent Office (USAIPO)

The U.S. Army Information Proponent Office (USAIPO) is charged to develop the capabilities and capacity across Army Doctrine, Organizations, Training and Education, Materials, Leadership, Personnel, and Facilities (DOTMLPF) that leverage the power of information to achieve mission success across the unified land operations.

As the U.S. Army Proponent Chief, the Commanding General, US Army Combined Arms Center (CG, CAC) established the IPO as a directorate within CAC Capabilities Development Integration Directorate to serve as his executive agent for accomplishing this critical mission. CAC-CDID is now subordinate to the Mission Command Center of Excellence (MC CoE), which was formally established on 15 September 2010. The major responsibilities of IPO are derived from CG, CAC's and MC-CoE priorities.

Mission of High Headquarters

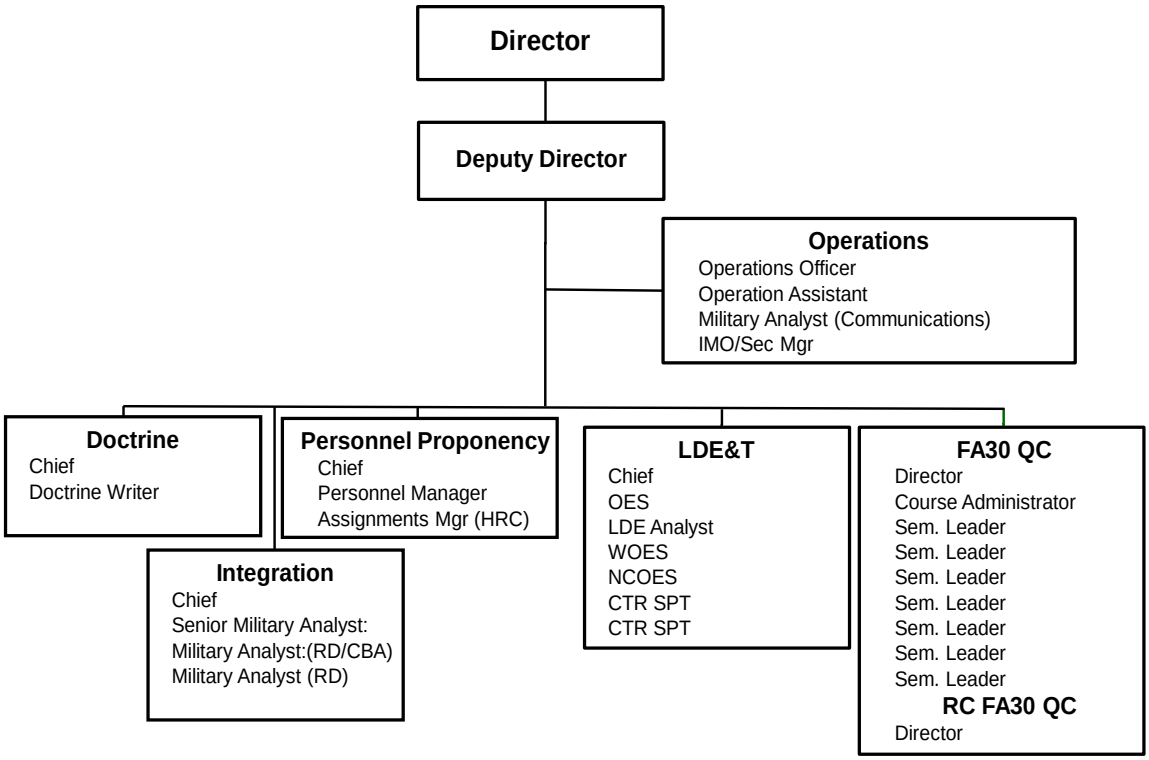
- **CAC Mission:** Provides leadership and supervision for the leader development and professional military and civilian education, institutional and collective training, functional training, training support, doctrine, lessons learned, battle command, and specified areas designated by CG, TRADOC.
- **MC CoE Mission:** Develops and integrates Mission Command DOTMLPF solutions at all levels of command in order to prepare leaders and their units to successfully conduct Unified Land Operations in a JIIM environment.

USAIPO Mission and Key Tasks: The mission and key tasks vision were approved by Director, CDID in October 2009.

- **Mission:** As directed, CAC CDID-IPO integrates capabilities and capacity across DOTMLPF to meet the Army's requirement for the successful planning, integration, and execution of Information Operations in full spectrum operations.
- **Key Tasks:**
    - Provide CAC Commander and CDID IO expertise and input to facilitate concept, requirements, and force modernization development as required.
    - Manage the U.S. Army's qualification courses for FA30 Officers (Active and Reserve Component).
    - Monitor, access, and integrate IO instruction within the Army's PME system.
    - Execute U.S. Army personnel life cycle management for FA30 officers IAW AR 600-3.
    - Develop IO doctrine and TTPs to support operational efforts.

USAIPO is organized as follows to accomplish this mission:

IPO Task Organization



Public Website: http://usacac.army.mil/cac2/IPO/index.asp

Updated: October 2011

Marine Corps Information Operations Center

Established 15 July 2009, the Marine Corps IO Center (MCIOC) is the Marine Corps' executive agent for the Marine Corps IO Program (MCIOP, MCO 3120.10) and the centralized repository of USMC IO expertise. The MCIOC augments the deployed MAGTF with scalable, mission-tailored IO Planning Teams (IOPTs), and Expeditionary MISO Detachments/Teams (EMD/T) during contingency operations, which require support that exceeds the MAGTF's organic IO capabilities. Additionally, the MCIOC directly supports Marine Forces during all phases of operations by providing training, mission planning, reach-back support, and coordination of USMC, Joint, Coalition and Interagency capabilities from the beginning of the planning cycle through completion of post deployment activities. The MCIOC also enables the development and integration of IO capabilities and doctrine throughout the Marine Corps.

Milestones: Recent MCIOC milestones include reaching full operational capability (FOC) in January 2011 and Command Designation in August 2011.

Mission: The Marine Corps Information Operations Center (MCIOC) provides operational support to the MAGTF and provides IO subject matter expertise in support of USMC IO advocates and proponents IOT enable the effective integration of IO into Marine Corps operations.

Marine Corps IO Center Support to the USMC:

1. Perform the duties of Executive Agent for the Marine Corps Information Operations Program.
2. Form, train, equip and deploy IO and MISO planning teams to augment supported unit organic staffs.
3. Form, train, equip and deploy tactical MISO delivery teams in support of deployed MAGTFs.
4. Maintain a single, fused, and continuously accessible Marine Corps IO reach-back capability that is fully integrated with relevant information and analysis sources.
5. Support the Marine Corps Advocate and Supporting Establishment in the development of IO and MISO personnel, equipment, and fiscal resources.
6. Sponsor the training, education, and retention of IO planners and MISO personnel in order to manage the USMC IO subject matter expertise.
7. Support DC CD&I the development of IO doctrine and DC PP&O with the development of IO policy.
8. Maintain functional relationships with all Joint, OSD, USG, and partner nation IO-related organizations.

Marine Corps IO Center Organization:
The MCIOC recently re-structured the organization to maintain three deployable IO Planning Teams (IOPTs), four Expeditionary MISO Detachments (EMDs), and a task-organized Regional Reach-back Element (RRE) to support operational MAGTF requirements:

- MCIOC IOPTs will be capable of simultaneously supporting up to one deployed MEF-size element and one deployed MEU, or three deployed MEUs. IOPTs will provide IO Planning SMEs to augment supported MAGTF IO cells. IO SMEs will support mission analysis and staff integration across IO core, supported and related capabilities in support of the commander's end state, to include analysis of the information environment, threat and nodal analysis, regional IO target expertise, measures of effectiveness development and analysis, and special technical operations planning.
- MCIOC EMDs will be capable of supporting up to a single MEF or three deployed MEUs with a tactical MISO delivery capability. EMD HQ will assist in mission analysis and COA development at the Brigade/Regiment-level while EMTs will do the same at the battalion level. EMTs will execute MISO series, advise the commander on the effects of their operations on the target audience, and provide focused tactical MISO support to the maneuver commander.
- MCIOC Regional Reach-back Element will establish communications internally, develop products, and leverage external resources to satisfy requests for information (RFIs) and disseminate timely, accurate and relevant information in order to support the MCIOC mission of providing IO support to the Marine Corps, Joint Forces and Coalition Partners. The RRE will task organize to provide prioritized support to deployed MAGTF IO cells, other USMC units and other DoD/Joint IO activities upon request.

The MCIOC S-2 (Intelligence) Division provides:

- Regional IO Intelligence Sections will integrate focused regional culture, media, political and threat intelligence into IO and MISO planning efforts and support the RRE and deployed IOPTs and EMD/Ts.
- The Intelligence Request Support Section will provide trans-regional terrorist expertise to support IO planning efforts and create, enhance and leverage targeting packages for Target Audiences, High Value Targets (HVTs), and High Value Individuals (HVIs) in the Information Environment.
- The Technical Analysis Section will support planning of Computer Network Operations and Electronic Warfare through development or enhancement of technical targeting packages.

Subordination: The Marine Corps IO Center is subordinate to Deputy Commandant for Plans, Policies and Operations (DC, PP&O). IOPTs and EPD/Ts will, in most cases, be attached to supported MAGTFs during operational deployments, including pre-deployment exercises via an established Request For Forces (RFF) process that is vetted and approved by DC, PP&O.

Leadership: The leadership of MCIOC consists of the Commander, a Colonel (O-6), the Chief of Staff, a GS-15, and the Senior Enlisted Advisor, a Sergeant Major (E-9).

Location: The IO Center is located aboard Marine Corps Base Quantico, VA.

For more information contact Mr. James McNeive at 703-784-5826 or email at jmcneive@mcia.osis.gov.

Updated: October 2011

Navy Information Operations Organizations

This section presents brief descriptions of selected U.S. Navy Information Operations organizations.

- The planned revision to NWP 3-13 Navy Information Operations have been placed on hold awaiting JP 3-13 ongoing revisions.
- When NWP 3-13 is completed the new document can be found at the Navy Doctrine Library System link: http://www.nwdc.navy.smil.mil

Fleet Cyber Command
The mission of Fleet Cyber Command is to direct Navy cyberspace operations globally to deter and defeat aggression and to ensure freedom of action to achieve military objectives in and through cyberspace; to organize and direct Navy cryptologic operations worldwide and support information operations and space planning and operations, as directed; to direct, operate, maintain, secure, and defend the Navy's portion of the Global Information Grid; to deliver integrated cyber, information operations cryptologic and space capabilities; and to deliver global Navy cyber network common cyber operational requirements.

Commander Tenth Fleet
The mission of Tenth fleet is to serve as the Number Fleet for Fleet Cyber Command and exercise operational control of assigned Naval forces; to coordinate with other naval, coalition and Joint Task Forces to execute the full spectrum of cyber, electronic warfare, information operations and signal intelligence capabilities and missions across the cyber, electromagnetic and space domains.

Navy Cyber Forces Command
Navy Cyber Forces Command (CYBERFOR) mission is to organize and prioritize, training, modernization, and maintenance, requirements, and capabilities of command and control architecture/networks, cryptologic and space-related systems and intelligence and information operations activities, and to coordinate with Type Commanders, to deliver interoperable, relevant and ready forces at the right time at the best cost, today and in the future. Navy Cyber Forces is the Type Commander for Navy's global cyber workforce of more than 14,000 Sailors and civilians. With a headquarters staff of nearly 600 located at Joint Expeditionary Base Little Creek-Fort Story, CYBERFOR provides ready forces and equipment in cryptology/signals intelligence, cyber, electronic warfare, information operations, intelligence, networks, and space.

Naval Network Warfare Command
Naval Network Warfare Command (NNWC) directs the operations and security of the Navy's portion of the Global Information Grid (GIG). NNWC delivers reliable and secure Net-Centric and Space war fighting capabilities in support of strategic, operational, and tactical missions across the Navy.

Navy Information Operations Command Norfolk
Navy Information Operations Command (NIOC) Norfolk, the Navy's Center of Excellence for IO, is responsible for providing operationally focused training; planning support and augmentation from the tactical to the strategic level; developing IO doctrine, tactics, techniques, and procedures; advocating requirements in support of future effects-based warfare; conducting experimentation for evaluating emerging or existing IO technologies and doctrine; providing and managing IO data for fleet operations.

Navy Cyber Defense Operations Command
The Navy Cyber Defense Operations Command (NCDOC) coordinates, monitors, and oversees the defense of Navy computer networks and systems, including telecommunications, and is responsible for accomplishing computer network defense (CND) missions as assigned by NAVNETWARCOM and USCYBERCOM.

Navy Cyber Warfare Development Group
Navy Cyber Warfare Development Group (NCWDG) serves as Navy's IO innovation center and functions as the principal technical agent for research and development of prototype IO capabilities. NIOC Suitland supports the development capabilities encompassing all aspects of IO attack, protect, and exploit; maintaining an aggressive program to acquire and analyze state-of-the-art technologies (software and hardware), evaluate fleet applicability, and prototype developmental capabilities. NCWDG maintains a collaborative relationship with Space and Naval Warfare Systems Command, Systems Center San Diego to provide efficient and effective technical expertise in command, control, communications, computers, and intelligence, surveillance, reconnaissance and information operations. NCWDG also supports development coordination between Fleet Cyber Command, Cyber Forces Command, OPNAV, NIOC Norfolk, systems commands, IO technology center, and the commercial industry.

Fleet Information Operations Center
Four regionally aligned Fleet Information Operations Centers provide IO planning and targeting support to their respective fleet commanders and strike group staffs.

Updated: October 2011

Air Force Intelligence, Surveillance and Reconnaissance Agency

The Air Force Intelligence, Surveillance and Reconnaissance Agency, with headquarters at Lackland Air Force Base, TX, was activated 8 June 2007. Formerly known as the Air Intelligence Agency, the new Air Force Intelligence, Surveillance and Reconnaissance Agency is aligned under the Air Force Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance as a Field Operating Agency.

Mission & Vision
The agency's mission is to deliver decisive advantage by providing and operating integrated cross-domain ISR capabilities in concert with service, joint, national, and international partners. Our vision is to be the preeminent ISR Enterprise providing the right ISR to the right person at the right time.

Personnel
The agency has almost 20,000 active, Reserve and Guard military and civilian members serving at 72 locations worldwide.

Organization
The 480th ISR Wing, 70th ISR Wing, 361st ISR Group, National Air and Space Intelligence Center and the Air Force Technical Applications Center are aligned under the Air Force ISR Agency. The agency is the Air Force's Service Cryptologic Element and is also responsible for mission management and support of signals intelligence operations for the 24th Air Force's 67th Network Warfare Wing and 688th Information Operations Wing, as well as the 12th Air Force's 55th Wing. In addition, the agency provides guidance to two Air Force Reserve and 22 Air National Guard units with ISR responsibilities. The Air Force ISR Agency further supplies mission management and support for specific intelligence operations within all of these organizations. Mission support includes organizing, training and equipping the service's cryptologic elements.

480th Intelligence, Surveillance and Reconnaissance Wing
The 480th ISR Wing at Joint Base Langley-Eustis AFB, VA, is the Air Force lead for developing timely and relevant ISR from a variety of platforms, 24 hours a day, year round, in direct support of combat operations, Air Force leaders, key Coalition partners and combatant commanders worldwide... Capabilities include global command and control for the collection, processing, exploitation and dissemination of ISR data from the U-2 "Dragon Lady," RQ-4 "Global Hawk," MQ-1 "Predator" and MQ-9 "Reaper," in addition to numerous other ISR platforms, using the Air Force Distributed Common Ground System weapon system. The wing also conducts real-time cryptologic and signals intelligence in direct support of combat operations and combatant commanders worldwide. The wing was activated 1 December 2003.

70th Intelligence, Surveillance and Reconnaissance Wing
The 70th ISR Wing at Fort George G. Meade, MD, integrates Air Force capabilities into global cryptologic operations, directly supporting national-level decision makers, combatant commanders and tactical warfighters. The wing works closely with the National Security Agency/Central Security Service, leveraging the net-centric capabilities of a worldwide cryptologic enterprise to conduct national missions and enable national-tactical integration for joint and combined Air Force combat operations around the world. The effect on battlespace is immediate, high-impact and decisive. The wing includes six intelligence groups in the U.S., Pacific and European theaters.

National Air and Space Intelligence Center (NASIC)
The National Air and Space Intelligence Center at Wright-Patterson AFB, OH, is the primary Department of Defense producer of foreign air and space intelligence. NASIC supports warfighters, force modernizers and national policy makers with world-class predictive intelligence products that integrate all available sources of intelligence data. The center analyzes the characteristics and performance of foreign weapons systems, assesses the capabilities and intent of potential adversaries, and serves as a national node for the processing, exploitation and dissemination of intelligence data from around the world. NASIC has four intelligence analysis groups and eighteen squadrons, all located in its main complex at Wright-Patterson AFB.

361st Intelligence, Surveillance and Reconnaissance Group
The 361st ISR Group at Hurlburt Field, FL is the premier provider of specialized ISR capabilities to the Air Force Special Operations Force community. They train, equip and present more than 250 Airmen to provide specialized SOF ISR forces for worldwide employment.

Air Force Technical Applications Center (AFTAC)
The Air Force Technical Applications Center at Patrick AFB, FL performs nuclear treaty monitoring and nuclear event detection. AFTAC provides national authorities quality technical measurements to monitor nuclear treaty compliance and performs research and development of new proliferation detection technologies to enhance or assist treaty verification to limit the proliferation of weapons of mass destruction to preserve our nation's security. AFTAC has been performing its nuclear event detection mission since its inception in 1973.

Point of Contact
Air Force ISR Agency, Commander's Action Group; 102 Hall Blvd, Ste 104; San Antonio, TX 78243-7089; DSN 969-4016 or (210) 977-4016.

Updated: September 2011

Headquarters 24th Air Force

The 24th Air Force (24 AF) is the Air Force's operational warfighting organization responsible for conducting the full range of Cyber operations. 24 AF establishes, operates, maintains and defends the Air Force provisioned portion of the DoD network to ensure the Joint Warfighter can maintain the information advantage while prosecuting military operations. Specifically, the 24 AF mission is to: Extend, operate and defend the Air Force portion of the DoD network and to provide full spectrum capabilities for the Joint warfighter in, through, and from Cyberspace.

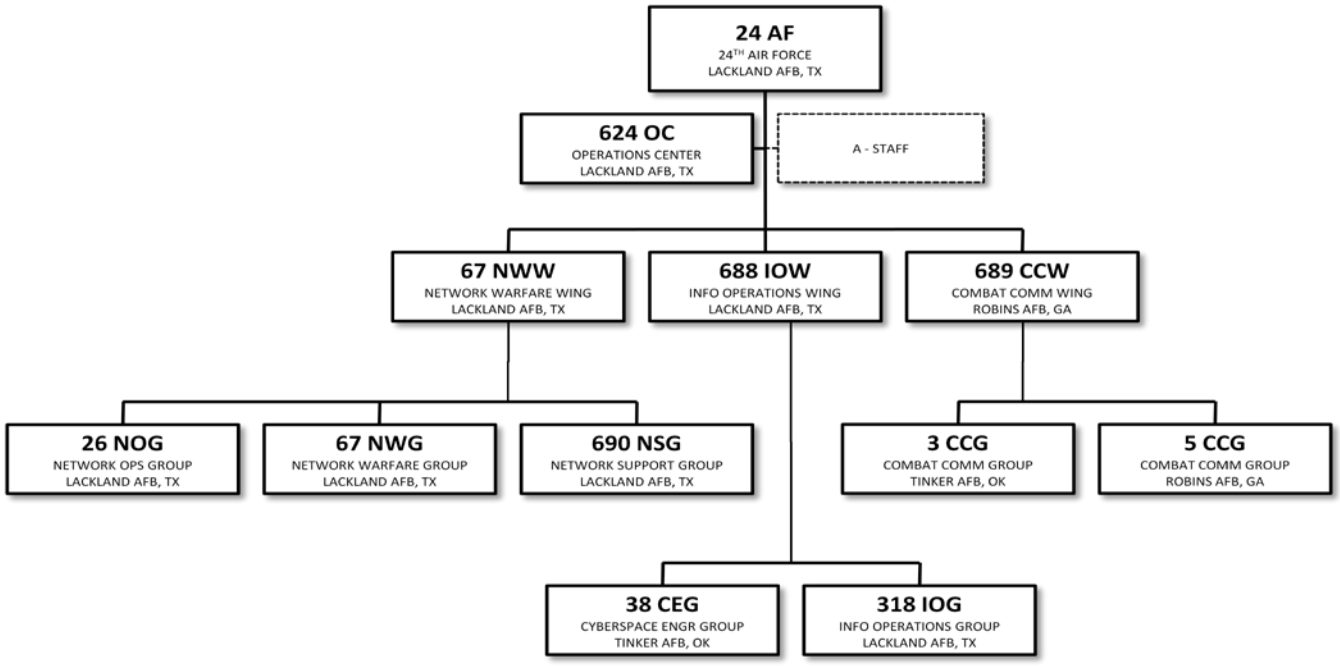
The 24 AF is subordinate to Air Force Space Command (AFSPC). AFSPC was assigned the Cyber mission (transferred from Air Combat Command) when 24 AF was established on 18 August 2009. AFSPC is 24 AF's "Organize, Train and Equip" entity, which advocates for personnel funding training and equipment to support the mission areas to enable 24 AF to meet operational mission requirements. AFSPC also provides administrative support, audit and inspections, financial management, manpower and organization, operational analysis, research and development, and training and education support to 24 AF.

Through its Joint chain, 24 AF presents Cyber forces to US Strategic Command, which has delegated operational control to US Cyber Command (USCYBERCOM) in Mod 9 to Operational Order 10-01 (21 May 10). Twenty-Fourth Air Force receives operational taskings through USCYBERCOM, which establishes 24 AF operational mission requirements. Additionally, 24 AF presents combat communications forces.

The Commander, 24 AF is also designated as the Air Force Network Operations Commander (AFNetOps/CC) with responsibility for the defense of the Air Force network. AFNetOps/CC authority is delegated through the AF administrative chain from the Secretary of the AF and grants the 24 AF/CC command authority of over 100 network control centers (NCCs) at AF bases and sites world-wide. NCCs are administratively assigned to AF squadrons, however, the 24 AF/CC issues them daily operational orders through the AFNetOps command and control structure for the daily defense and operation of the AF network.

The 24 AF is located at Lackland AFB, TX and has three subordinate wings (the 67th Network Warfare Wing (67 NWW), located at Lackland AFB, TX, the 688th Information Operations Wing (688 IOW), also located at Lackland AFB, TX, and the 689th Combat Communications Wing (689 CCW) at Robins AFB, Georgia) and the 624th Operations Center, at Lackland AFB, TX. The 24 AF oversees 5,400 Airmen to conduct or support 24-hour operations involving Cyberspace operations, including 3,337 military, 775 civilian and 1,364 contractor personnel. In addition, more than 10,000 Air National Guard and Air Force Reserve personnel are aligned to support the 24AF and AFSPC mission.

Organization:



Point of Contact:
24th Air Force Public Affairs, 467 Moore Street, Bldg. 2167, Lackland AFB, TX, CML 210-395-7020, DSN 969-7020.

Updated: October 2011

624th Operations Center

The 24 AF executes command and control over the AFNet and AF Cyber forces through the 624 Operations Center. The 624 OC is the single inject point for operational Cyber taskings for the AF. The 624 OC's organizational structure is aligned with its operational counterparts (AOCs) to facilitate integration of 24 AF capabilities into the supported CCDR's existing structure. The 624 OC consists of the following four divisions:

- Strategy Division (SRD): Formulates the overarching campaign guidance/strategy through the Cyber Operations Directive (CyOD)…analogous to the AOC's Air Operations Directive…to align the 24 AF/CC's priorities in support of HHQ directives/ objectives. The related timeline for SRD issues is 72+ hours. SRD hands off the strategic guidance to the Combat Plans Division to enable planning and execution.
- Combat Plans Division (CPD): Works with its AOC counterpart to synchronize the employment of 24 AF full spectrum cyber capabilities with the AOC's Air Tasking Order (ATO) and Airspace Control Order (ACO). The timeline for CPD actions is the next 24-48 (tomorrow's war). 624 OC/CPD produces the AF Cyber Tasking Order (AF CTO)… analogous to the ATO…the Cyberspace Control Order (CCO)…analogous to the ACO…and related Special Instructions (SPINS) are handed off to the Combat Operations Division for execution during the following day's operations.
- Combat Operations Division (COD): Monitors the execution of the AF CTO and CCO, maintains up-to-date situational awareness of the defensive posture of the Air Force Information Network (AFIN), and is the focal point of all communications into and out of the 624 OC. Adjusts tasking real-time if possible (based on asset availability).
- Intelligence, Surveillance, Reconnaissance Division (ISRD): Focuses on the "near fight" – defines potential threats to AFIN operations in the 72 hour AF CTO time frame (crisis/adaptive planning operations).

The 624 OC conducts adaptive and crisis action planning. As a result of that planning process, the 624 OC issues orders on behalf of the 24 AF/CC. These "Cyber" orders have been adapted from the AOC process, mirroring similar orders from the Space Operations Center and theater AOCs.

The 624 OC also concentrates all of the authorities established in the United States Code required to perform Cyber operations. As events occur in Cyberspace, and operators respond, ambiguity can arise as to whether a situation is most appropriately handled by law enforcement (Title 18), counter-intelligence (Title 50), or armed forces (Title 10). If additional information becomes available, which indicates a change in the most appropriate authority, crucial time could be lost while operators contact counterparts and perform handoff. Instead, 24 AF has developed relationships with Title 18 and Title 50 counterparts, which perform duty on the 624 OC floor. If a situation transitions from one authority to another, the 624 OC can react appropriately in real-time. 24 AF and 624 OC also rely heavily on the Air Reserve Component for operational capacity and includes Title 32 capabilities in the 624 OC as well.

Updated: October 2011

This Page Intentionally Blank

67th Network Warfare Wing

The 67th Network Warfare Wing (67 NWW) executes the integrated planning and employment of military capabilities to achieve the desired effects across the interconnected analog and digital portion of the Battlespace—Air Force Network Ops. The Wing's Cyber Warriors conduct network operations through the dynamic combination of hardware, software, data, and human interaction that involves time-critical, operational-level decisions that direct configuration changes and information routing.

The 67 NWW, headquartered at Lackland AFB, TX, is the Air Force's only Network Warfare Wing. The wing employs 2,500 military and civilian Air Force Space Command personnel in 25 locations worldwide. As the 24 AF's execution arm for AF Net Ops, the wing readies and employs Airmen to conduct network defense and full spectrum network ops and systems telecommunications monitoring for AF and combatant commanders.

The wing consists of the 67th Network Warfare Group, 26th Network Operations Group, and 690th Network Support Group. Activated in 1947, the wing conducted Tactical Reconnaissance and later was the only wing of its type in Korea during the Korean War. The wing later trained Air Force and other countries' aircrews in the RF-4C Phantom. One squadron of the wing saw combat action during Operations DESERT SHIELD and DESERT STORM. In 1993, the Wing was redesignated as the 67th Intelligence Wing and was the largest wing in the Air Force at the time. In 2000, the wing was assigned the mission of Information Operations becoming the Air Force's first IO Wing. In July 2006, the wing became the Air Force's first and only Network Warfare Wing executing the Cyber portion of the Air Force mission to Fly, Fight, and Win in Air, Space and Cyberspace.

Updated: October 2011

This Page Intentionally Blank

688th Information Operations Wing

The 688th Information Operations Wing (688 IOW) is located at Lackland AFB, San Antonio, TX. The wing's mission statement is: Deliver proven Information Operations and Engineering Infrastructure capabilities integrated across air, space and cyberspace domains. The wing was formally designated on 18 August 2009. The 688 IOW was originally activated as the 6901st Special Communication Center in July 1953, and became the Air Force Electronic Warfare Center in 1975. Air Force successes in exploiting enemy information systems during Operation Desert Storm led to the realization that the strategies and tactics of command and control warfare could be expanded to the entire information spectrum and be implemented as information warfare. In response, the Air Force Information Warfare Center (AFIWC) was activated on 10 September 1993, combining technical skill sets from the former Air Force Electronic Warfare Center (AFEWC) with the Air Force Cryptologic Support Center's Securities Directorate and intelligence capabilities from the former Air Force Intelligence Command. On 1 October 2006, AFIWC was re-designated the Air Force Information Operations Center (AFIOC). The name was changed to better reflect the center's continued advancements in network warfare, electronic warfare and influence operations missions. AFIOC was re-designated as the 688 IOW on 18 August 2009 and aligned under 24th Air Force.

The wing is composed of two groups: the 318th Information Operations Group (IOG) at Lackland AFB and the 38th Cyberspace Engineering Group (CEG) at Tinker AFB. The 318 IOG explores new cyberspace technologies to engineer next-generation weapons capabilities for operational warfighters. It has a test squadron for developmental and operational test and evaluation, a tactics squadron to optimize IO tactics, techniques, and procedures for weapon systems, a school house to arm the next generation of cyber warriors with the most up-to-date information, and an assessment squadron to identify and mitigate vulnerabilities on AF systems.

The 38 CEG is the Air Force's premier Engineering and Installation group, providing systems telecommunications managers to every Combatant Command, Major Command, and Air Force base worldwide. The unit provides communications infrastructure installations and services, to include cable and antenna systems, electronic systems, specialized engineering electromagnetic interference testing, radio frequency and radiation Hazard surveys and high-altitude electromagnetic pulse protection verification. Additionally, the 85th EIS is the AF's only Designed Operations Capability (DOC) tasked Engineering and Installation rapid response force.

The wing's team of more than 1200 military and civilian members is skilled in the areas of engineering installation, weaponeering, operations research, intelligence, communications and computer applications.

Updated: September 2011

This Page Intentionally Blank

689th Combat Communications Wing

The 689th Combat Communications Wing (689 CCW) is located at Robins Air Force Base, Warner Robins, Georgia. The 689 CCW's mission statement: Deliver combat communications for the joint/coalition war fighter supporting combat operations and Humanitarian Relief Operations…anytime…anywhere!

The unit traces it linage to the 1931st Airways and Air Communications Squadron, which was originally designated in 1948. It was later re-designated as the 1931st Communications Squadron in 1961. Then, in 1969, the squadron grew and was again re-designated as the 1931st Communications Group. The 1931st would go through several more re-designations due to the demands of the Air Force before finally being de-activated on 26 September 1991. During its lifespan, the 1931st served with distinction in the Alaskan Communications region, Air Force Communications Command, 21st Fighter Wing. The distinguished service of the 1931st was recognized with the award of the Air Force Outstanding Unit Award eight times. The wing resumed its history and was reactivated and redesignated on 5 October 2009 as the 689 CCW under 24th Air Force and Air Force Space Command.

The 689 CCW has brought together, as one cohesive team, several active and reserve subordinate units with their own storied histories and over 150 major awards. Active Duty units include the 3rd Combat Communications Group and the 5th Combat Communications Group. Air National Guard partners consist of the 162nd, 201st, 226th, 251st, 252nd, 253rd, 254th, and 281st Combat Communications Groups and the 224th and 290th Joint Communications Support Squadrons. Air Force Reserve units include 23rd Combat Communications Squadron, 35th Combat Communications Squadron, 42nd Combat Communications Squadron, and 55th Combat Communications Squadron.

The Wing current has a war time projection force of more than 6,000 skilled Airmen (1,500 AD & 4,500 ARC), armed with over $600 million dollars worth of materiel, who provide tactical communications, computer systems, navigational aids, and Air Traffic Control (ATC) services anywhere in the world to meet the Air Force, Department of Defense, and other US Commitments. Total Force Team members, including DoD civilians and contractors, are trained to deploy more than 150 mission systems providing initial services to deployed customers at various units under hostile conditions in austere locations where communications and ATC capabilities are not established.

Updated: October 2011

This Page Intentionally Blank

Glossary

Most terms are taken from the Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms* (8 November 2010, as amended through 15 September 2011).

Area of interest (AOI) - That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory to the objectives of current or planned operations. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission. (JP 1-02)

Civil affairs (CA) - Designated Active and Reserve component forces and units organized, trained, and equipped specifically to conduct civil affairs activities and to support civil-military operations. (JP 1-02)

Civil military operations (CMO) - The activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to facilitate military operations, to consolidate and achieve operational US objectives. Civil-military operations may include performance by military forces of activities and functions normally the responsibility of the local, regional, or national government. These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed, in the absence of other military operations. Civil-military operations may be performed by designated civil affairs, by other military forces, or by a combination of civil affairs and other forces. (JP 1-02)

Combat Camera (COMCAM) - The acquisition and utilization of still and motion imagery in support of operational and planning requirements across the range of military operations and during joint exercises. (JP 1-02)

Command and control (C2) - The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (JP1- 02)

Command and control system - The facilities, equipment, communications, procedures, and personnel essential for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned. (JP 1-02)

Computer network attack (CNA) - Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (JP 1-02)

Computer network defense (CND) - Actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks. (JP 1-02)

Computer network exploitation (CNE) - Enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks. (JP 1-02)

Computer network operations (CNO) - Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. (JP 1-02)

Computer security (COMPUSEC) - The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems. (JP 1-02)

Counterdeception - Efforts to negate, neutralize, diminish the effects of, or gain advantage from a foreign deception operation. Counterdeception does not include the intelligence function of identifying foreign deception operations. (JP 1-02)

Counterintelligence - The information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassination conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (JP 1-02)

Counterpropaganda - (Army) Programs of products and actions designed to nullify propaganda or mitigate its effects. (FM 3-13)

Cyber counterintelligence - Measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligences service collection efforts that use traditional methods to gauge cyber capabilities and intentions. (JP1-02)

Cyberspace - A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (CJCS CM-0363-08) (JP 1-02)

Cyberspace operations - The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. (JP 1-02)

Deception action - A collection of related deception events that form a major component of a deception operation. (JP 1-02)

Deception concept - The deception course of action forwarded to the Chairman of the Joint Chiefs of Staff for review as part of the combatant commander's strategic concept. (JP 1-02)

Deception course of action - A deception scheme developed during the estimate process in sufficient detail to permit decision-making. At a minimum, a deception course of action will identify the deception objective, the deception target, the desired perception, the deception story, and tentative deception means. (JP 1-02)

Deception event - A deception means executed at a specific time and location in support of a deception operation. (JP 1-02)

Deception means - Methods, resources, and techniques that can be used to convey information to the deception target. There are three categories of deception means: a. physical means. Activities and resources used to convey or deny selected information to a foreign power. b. technical means. Military materiel resources and their associated operating techniques used to convey or deny selected information to a foreign power. c. administrative means. Resources, methods, and techniques to convey or deny oral, pictorial, documentary, or other physical evidence to a foreign power. (JP 1-02)

Deception objective - The desired result of a deception operation expressed in terms of what the adversary is to do or not to do at the critical time and/or location. (JP 1-02)

Deception story - A scenario that outlines the friendly actions that will be portrayed to cause the deception target to adopt the desired perception. (JP 1-02)

Deception target - The adversary decision maker with the authority to make the decision that will achieve the deception objective. (JP 1-02)

Defense support to public diplomacy (DSPD) - Those activities and measures taken by the Department of Defense components to support and facilitate public diplomacy efforts of the United States Government. (JP 1-02)

Desired perception - In military deception, what the deception target must believe for it to make the decision that will achieve the deception objectives. (JP 1-02)

Disinformation - (Army) Information disseminated primarily by intelligence organizations or other covert agencies designed to distort information, or deceive or influence United States decisionmakers, United States forces, coalition allies, key actors, or individuals by indirect or unconventional means. (FM 3-13)

DOD - Department of Defense (JP 1-02)

DODD - Department of Defense directive (JP 1-02)

Electromagnetic pulse (EMP) - The electromagnetic radiation from a strong electronic pulse, most commonly caused by a nuclear explosion that may couple with electrical or electronic systems to produce damaging current and voltage surges. (JP 1-02)

Electromagnetic spectrum - The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. (JP 1-02)

Electronics security - The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of non communications electromagnetic radiation, e.g., radar. (JP 1-02)

Electronic warfare (EW) - Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Electronic warfare consists of three divisions: electronic attack, electronic protection, and electronic warfare support.

- **electronic attack (EA)** - Division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires.
- **electronic protection (EP)** - Division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability.
- **electronic warfare support (ES)** - Division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. (JP 1-02)

Global Information Grid (GIG) - The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems. (JP 1-02)

Global information infrastructure (GII) - The worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The global information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers,

switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the global information infrastructure. (JP 1-02)

High-payoff target (HPT) - A target whose loss to the enemy will significantly contribute to the success of the friendly course of action. High-payoff targets are those high-value targets, identified through war-gaming, that must be acquired and successfully attacked for the success of the friendly commander's mission. (JP 1-02)

High-value target (HVT) - A target the enemy commander requires for the successful completion of the mission. The loss of high-value targets would be expected to seriously degrade important enemy functions throughout the friendly commander's area of interest. (JP 1-02)

Human factors - The psychological, cultural, behavioral, and other human attributes that influence decision-making, the flow of information, and the interpretation of information by individuals or groups. (JP 1-02)

Influence operations - (Air Force) Employment of capabilities to affect behaviors, protect operations, communicate commander's intent, and project accurate information to achieve desired effects across the cognitive domain. These effects should result in differing behavior or a change in the adversary decision cycle, which aligns with the commander's objectives. (AFDD 3-13)

Information - 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)

Information assurance (IA) - Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (JP1-02)

Information environment - The aggregate of individuals, organizations or systems that collect, process, or disseminate information. (JP 1-02)

Information management (IM) - The function of managing an organization's information resources for the handling of data and information acquired by one or many different systems, individuals, and organizations in a way that optimizes access by all who have a share in that data or a right to that information. (JP 1-02)

Information operations (IO) - The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. (JP 1-02)

IO capability specialist - A functional expert in one or more of the IO core capabilities. They serve primarily in their specialty areas but may also serve as IO planners after receiving IO planner training. (DODI 3608.11)

IO career force - The military professionals that perform and integrate the core IO capabilities. The IO Career Force consists of IO Capability Specialists and IO Planners. (DODI 3608.11)

IO planner - A functional expert trained and qualified to execute full spectrum IO. They usually serve one or more tours as an IO capability specialist prior to assignment as an IO planner and may hold non-IO positions throughout their careers. (DODI 3608.11)

INFOCON - Information Operations Condition (JP 1-02)

Information security (INFOSEC) - The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. (JP 1-02)

Information superiority - The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (JP 1-02)

Information systems - The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. (JP 1-02)

Intelligence - The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity. (JP 1-02)

Interagency coordination - Within the context of Department of Defense involvement, the coordination that occurs between elements of Department of Defense, and engaged US Government agencies and departments for the purpose of achieving an objective. (JP 1-02)

Joint intelligence preparation of the operational environment (JIPOE) - The analytical process used by joint intelligence organizations to produce intelligence estimates and other intelligence products in support of the joint force commander's decision-making process. It is a continuous process that includes defining the operational environment; describing the impact of the operational environment; evaluating the adversary; and determining adversary courses of action. (JP 1-02)

Joint restricted frequency list (JRFL) - A time and geographically-oriented listing of TABOO, PROTECTED, and GUARDED functions, nets, and frequencies. It should be limited to the minimum number of frequencies necessary for friendly forces to accomplish objectives.

- **Taboo frequencies** - Any friendly frequency of such importance that it must never be deliberately jammed or interfered with by friendly forces. Normally, these frequencies include international distress, CEASE BUZZER, safety, and controller frequencies. These frequencies are generally long standing. However, they may be time-oriented in that, as the combat or exercise situation changes, the restrictions may be removed. (JP 1-02)
- **Protected frequencies** - Those friendly frequencies used for a particular operation, identified and protected to prevent them from being inadvertently jammed by friendly forces while active electronic warfare operations are directed against hostile forces. These frequencies are of such critical importance that jamming should be restricted unless absolutely necessary or until coordination with the using unit is made. They are generally time-oriented, may change with the tactical situation, and must be updated periodically.
- **Guarded frequencies** - Enemy frequencies that are currently being exploited for combat information and intelligence. A guarded frequency is time-oriented in that the guarded frequency list changes as the enemy assumes different combat postures. These frequencies may be jammed after the commander has weighed the potential operational gain against the loss of the technical information.

Joint targeting coordination board (JTCB) - A group formed by the joint force commander to accomplish broad targeting oversight functions that may include but are not limited to coordinating targeting information, providing targeting guidance and priorities, and refining the

joint integrated prioritized target list. The board is normally comprised of representatives from the joint force staff, all components and, if required, component subordinate units. (JP 1-02)

Measure of effectiveness (MOE) - A criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect. (JP 1-02)

Military deception (MILDEC) - Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. (JP 1-02)

Military information support operations (MISO) - Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of military information support operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. (JP 1-02)

Network Operations (NETOPS) - 1. Activities conducted to operate and defend the Global Information Grid. (JP 1-02). 2. The DOD-wide operational, organizational, and technical capabilities for operating and defending DOD information networks. NETOPS includes, but is not limited to, enterprise management, net assurance, and content management. (JP 3-0)

Nongovernmental organization (NGO) - A private, self-governing, not-for-profit organization dedicated to alleviating human suffering; and/or promoting education, health care, economic development, environmental protection, human rights, and conflict resolution; and/or encouraging the establishment of democratic institutions and civil society. (JP 1-02)

Operations security (OPSEC) - A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. identify those actions that can be observed by adversary intelligence systems; b. determine indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. (JP 1-02)

Perception management - (Army) Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning; and to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover, deception, and psychological operations. (FM 3-13)

Physical destruction - (Army) The application of combat power to destroy or neutralize adversary forces and installations. It includes direct and indirect forces from ground, sea, and air forces. Also included are direct actions by special operations forces. (FM 3-13)

Physical security - 1. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. 2. **In communications security**, the component that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (JP1-02)

Priority national intelligence objectives - A guide for the coordination of intelligence collection and production in response to requirements relating to the formulation and execution of national

security policy. They are compiled annually by the Washington Intelligence Community and flow directly from the intelligence mission as set forth by the National Security Council. They are specific enough to provide a basis for planning the allocation of collection and research resources, but not so specific as to constitute in themselves research and collection requirements. (JP 1-02)

Propaganda - Any form of adversary communication, especially of a biased or misleading nature, designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly. (JP 1-02)

Psychological operations (PSYOP) - This term has been replaced by Military information support operations (MISO).

Public affairs (PA) - Those public information, command information, and community engagement activities directed toward both the external and internal publics with interest in the DOD. (JP 1-02)

Public diplomacy (PD) - 1. Those overt international public information activities of the United States Government designed to promote United States foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers, and by broadening the dialogue between American citizens and institutions and their counterparts abroad. 2. In peace building, civilian agency efforts to promote an understanding of the reconstruction efforts, rule of law, and civic responsibility through public affairs and international public diplomacy operations. Its objective is to promote and sustain consent for peace building both within the host nation and externally in the region and in the larger international community. (JP 1-02)

Public information - Within public affairs, that information of a military nature, the dissemination of which is consistent with security and approved for release. (JP 1-02)

Reachback - The process of obtaining products, services, and applications, or forces, or equipment, or material from organizations that are not forward deployed. (JP 1-02)

Strategic communication (SC) - Focused United States Government efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of United States Government interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power. (JP 1-02)

Target audience (TA) - An individual or group selected for influence. (JP 1-02.)

The Dictionary of Military and Associated Terms is available on line at: http://www.dtic.mil/doctrine/dod_dictionary/

Updated: November 2011

This Page Intentionally Blank

Information Operations, Cyberspace, and Strategic Communication Related Websites

The appearance of hyperlinks to civilian enterprises does not constitute endorsement by the U.S. Army of the web site or the information, products or services contained therein. Also be aware that for other than authorized activities such as military exchanges and Morale, Welfare and Recreation sites, the U.S. Army does not exercise any editorial control over the information you may find at these locations. These links are provided as a reference for the readers of the IO Primer.

United States Army War College: DIME – Information as Power - http://www.carlisle.army.mil/DIME/

United States Army War College: Information as Power Blog Site - http://www.carlisle.army.mil/DIME/blog/default.cfm?blog=dime

Information Operations and Cyberspace Related Websites:

Air Force Institute of Technology: Center for Cyberspace Research - http://www.afit.edu/en/ccr/index.cfm

Air University: Cyber Space and Information Operations Study Center - http://www.au.af.mil/info-ops/index.htm

Army: 1st Information Operations Command (Land) - http://www.inscom.army.mil/MSC/Default1st.aspx?text=off&size=12pt

Army: Chief Information Officer/G6 - http://ciog6.army.mil/

Army Combined Arms Center: Electronic Warfare Proponent Office (EWPO) - http://usacac.army.mil/cac2/cew/index.asp

Army Communicator (U.S. Army Signal Regiment's professional magazine) - http://www.signal.army.mil/ArmyCommunicator/AC.aspx

Center for Technology and National Security Policy - http://www.ndu.edu/ctnsp/

Commission on Cyber Security for the 44th Presidency - http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

Common Vulnerabilities and Exposures - http://cve.mitre.org/cve/index.html

Cyberdeterrence and Cyberwar: RAND Report by Martin C. Libicki (2009) - http://www.rand.org/pubs/monographs/MG877/

Cyber Power by Joseph Nye, Jr. (May 2010) - http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf

Cyberspace (High Frontier - The Journal for Space and Missile Professionals), May 2009 - http://www.afspc.af.mil/shared/media/document/AFD-090519-102.pdf

Cyberspace Sciences and Information Intelligence Research - http://www.ioc.ornl.gov/

DHS: National Cyber Security Division - http://www.dhs.gov/xabout/structure/editorial_0839.shtm

DHS: National Infrastructure Advisory Council - http://www.dhs.gov/files/committees/editorial_0353.shtm

DoD: High Performance Computing Modernization Program - http://www.hpcmo.hpc.mil/index.html

DoD: Strategy for Operating in Cyberspace (July 2011) - http://www.defense.gov/news/d20110714cyber.pdf

Emerging Cyber Threats Report 2012 (Georgia Tech) - http://www.gtisc.gatech.edu/doc/emerging_cyber_threats_report2012.pdf

Global Trends 2025 A Transformed World (National Intelligence Council) - http://www.dni.gov/nic/PDF_2025/2025_Global_Trends_Final_Report.pdf

Information Warfare Monitor – Tracking Cyberpower - http://www.infowar-monitor.net/

IO Journal (official publication of the Information Operations Institute, Association of Old Crows) - http://www.crows.org/the-io-institute/io-journal.html

Journal of Electronic Defense (official publication of the Association of Old Crows) - http://www.crows.org/jed/jed.html

Long War Journal - http://www.longwarjournal.org/

National Cyber Security Research and Development Challenges Related to Economics, Physical Infrastructure and Human Behavior (2009) - http://www.thei3p.org/docs/publications/i3pnationalcybersecurity.pdf

National Institute of Standards and Technology (NIST): Computer Security Division - Computer Security Resource Center - http://csrc.nist.gov/

National Institute of Standards and Technology (NIST): Information Technology Lab - http://www.nist.gov/itl/

National Vulnerability Database - http://web.nvd.nist.gov/view/vuln/search?execution=e1s1

Navy Center for Applied Research in Artificial Intelligence - http://www.nrl.navy.mil/aic/

Reviewing the Federal Cybersecurity Mission: Statement to the U.S. House of Representatives Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology (10 Mar 2009) - http://csis.org/files/media/csis/congress/ts090310_lewis.pdf

Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities - http://www.nap.edu/catalog.php?record_id=12651

U.S. Computer Emergency Readiness Team (US-CERT) - http://www.us-cert.gov/control_systems/csthreats.html

U.S. House of Representatives: Subcomittee on Emerging Threats, Cybersecurity, and Science and Technology - http://homeland.house.gov/subcommittee-3

U.S. International Strategy for Cyberspace (May 2011) - http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf

Strategic Communication Related Websites:

American Forces Press Service (DoD Website) - http://www.defense.gov/news/

COMOPS Monitor - http://comops.org/monitor/

Consortium for Strategic Communication - http://www.comops.org/

Defense Information School: The Center of Excellence for Visual Information and Public Affairs - http://www.dinfos.osd.mil/

Joint Forces Staff College - Strategic Communication Bibliography - http://www.jfsc.ndu.edu/library/publications/bibliography/strategic_communication.asp

Kaboom: A Soldier's War Journal (archived) - http://kaboomwarjournalarchive.blogspot.com/

Public Diplomacy Alumni Association - http://www.publicdiplomacy.org/

South East European Times - http://www.setimes.com/

The News & Views of the Maghreb - http://www.magharebia.com/cocoon/awi/xhtml1/en_GB/homepage/

The Washington Institute for Near East Policy - http://www.washingtoninstitute.org/templateI01.php

Under Secretary of State for Public Diplomacy and Public Affairs - http://www.state.gov/r/

UPENN Annenberg School for Communication - http://www.asc.upenn.edu/

USC Annenberg School for Communication - http://annenberg.usc.edu/

USC Center on Public Diplomacy - http://uscpublicdiplomacy.org/

Wisdom and Strength for the Future

"Not to promote war,
but to preserve peace..."